Hughes Hubbard & Reed

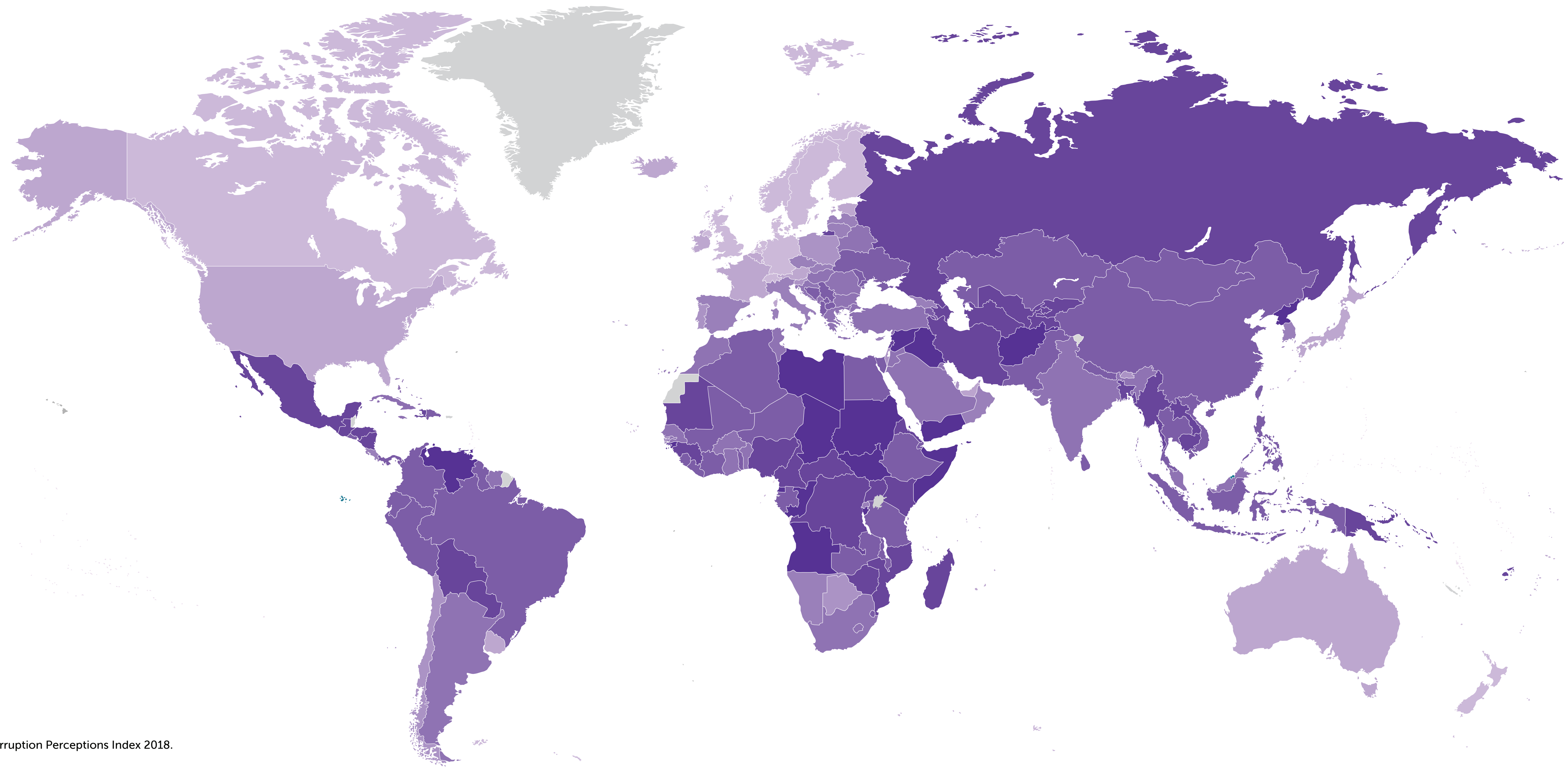
Fall 2019

alert

FCPA & Anti-Bribery

Hughes Hubbard & Reed LLP
A New York Limited Liability Partnership • One Battery Park Plaza
New York, New York 10004-1482 • +1 (212) 837-6000

Hughes Hubbard & Reed



CORRUPTION PERCEPTION SCORE

No Data

100 Very Clean

50

0 Very Corrupt

Data from Transparency International's Corruption Perceptions Index 2018.

SCORE	COUNTRY/TERRITORY	RANK
88	Denmark	1
87	New Zealand	2
85	Finland	3
85	Singapore	3
85	Sweden	3
85	Switzerland	3
84	Norway	7
82	Netherlands	8
81	Canada	9
81	Luxembourg	9
80	Germany	11
80	United Kingdom	11
77	Australia	13
76	Austria	14
76	Hong Kong	14
76	Iceland	14
75	Belgium	17
73	Estonia	18
73	Ireland	18
73	Japan	18
72	France	21
71	United States	22
70	United Arab Emirates	23
70	Uruguay	23
68	Barbados	25
68	Bhutan	25
67	Chile	27
66	Seychelles	28
65	Bahamas	29
64	Portugal	30
63	Brunei Darussalam	31
63	Taiwan	31
62	Qatar	33
61	Botswana	34
61	Israel	34
60	Poland	36
60	Slovenia	36
59	Cyprus	38
59	Czech Republic	38
59	Lithuania	38
58	Georgia	41
58	Latvia	41
58	Saint Vincent and the Grenadines	41
58	Spain	41
57	Cabo Verde	45
57	Dominica	45
57	South Korea	45
56	Costa Rica	48
56	Rwanda	48
55	Saint Lucia	50
54	Malta	51
53	Namibia	52
52	Grenada	53
52	Italy	53
52	Oman	53
51	Mauritius	56
50	Slovakia	57
49	Jordan	58
49	Saudi Arabia	58
48	Croatia	60
47	Cuba	61
47	Malaysia	61
47	Romania	61
46	Hungary	64
46	Sao Tome and Principe	64
46	Vanuatu	64
45	Greece	67
45	Montenegro	67
45	Senegal	67
44	Belarus	70
44	Jamaica	70
44	Solomon Islands	70
43	Morocco	73
43	South Africa	73
43	Suriname	73
43	Tunisia	73
42	Bulgaria	77
41	Burkina Faso	78
41	Ghana	78
41	India	78
41	Kuwait	78
41	Lesotho	78
41	Trinidad and Tobago	78
41	Turkey	78
40	Argentina	85
40	Benin	85
39	China	87
39	Serbia	87
38	Bosnia and Herzegovina	89
38	Indonesia	89
38	Sri Lanka	89
38	Swaziland	89
37	Gambia	93
37	Guyana	93
37	Kosovo	93
37	Macedonia	93
37	Mongolia	93
37	Panama	93
36	Albania	99
36	Bahrain	99
36	Colombia	99
36	Philippines	99
36	Tanzania	99
36	Thailand	99
35	Algeria	105
35	Armenia	105
35	Brazil	105
35	Côte d'Ivoire	105
35	Egypt	105
35	El Salvador	105
35	Peru	105
35	Timor-Leste	105
35	Zambia	105
34	Ecuador	114
34	Ethiopia	114
34	Niger	114
33	Moldova	117
33	Pakistan	117
33	Vietnam	117
32	Liberia	120
32	Malawi	120
32	Mali	120
32	Ukraine	120
31	Djibouti	124
31	Gabon	124
31	Kazakhstan	124
31	Maldives	124
31	Nepal	124
30	Dominican Republic	129
30	Sierra Leone	129
30	Togo	129
29	Bolivia	132
29	Honduras	132
29	Kyrgyzstan	132
29	Laos	132
29	Myanmar	132
29	Paraguay	132
28	Guinea	138
28	Iran	138
28	Lebanon	138
28	Mexico	138
28	Papua New Guinea	138
28	Russia	138
27	Comoros	144
27	Guatemala	144
27	Kenya	144
27	Mauritania	144
27	Nigeria	144
26	Bangladesh	149
26	Central African Republic	149
26	Uganda	149
25	Azerbaijan	152
25	Cameroon	152
25	Madagascar	152
25	Nicaragua	152
25	Tajikistan	152
24	Eritrea	157
23	Mozambique	158
23	Uzbekistan	158
22	Zimbabwe	160
20	Cambodia	161
20	Democratic Republic of the Congo	161
20	Haiti	161
20	Turkmenistan	161
19	Angola	165
19	Chad	165
19	Congo	165
18	Iraq	168
18	Venezuela	168
17	Burundi	170
17	Libya	170
16	Afghanistan	172
16	Equatorial Guinea	172
16	Guinea Bissau	172
16	Sudan	172
14	North Korea	176
14	Yemen	176
13	South Sudan	178
13	Syria	178
10	Somalia	180

Anti-Corruption and Internal Investigations Practice Group

PARTNERS

Kevin T. Abikoff

Derek J.T. Adler

Robert B. Bell

Benjamin S. Britz

Roel C. Campos

Charles W. Cohen

Diego Durán de la Vega

Ryan Fayhee

Anne Gaustad

Terence Healy

Michael H. Huneke

Salim Jorge Saud Neto*

Matthew R. Nicely

Neil J. Oxford

Eric S. Parnes

Laura N. Perkins

Bryan J. Sillaman

Elizabeth Solander

Nicolas Swerdloff

Nicolas Tollet

George A. Tsougarakis

Marc A. Weinstein

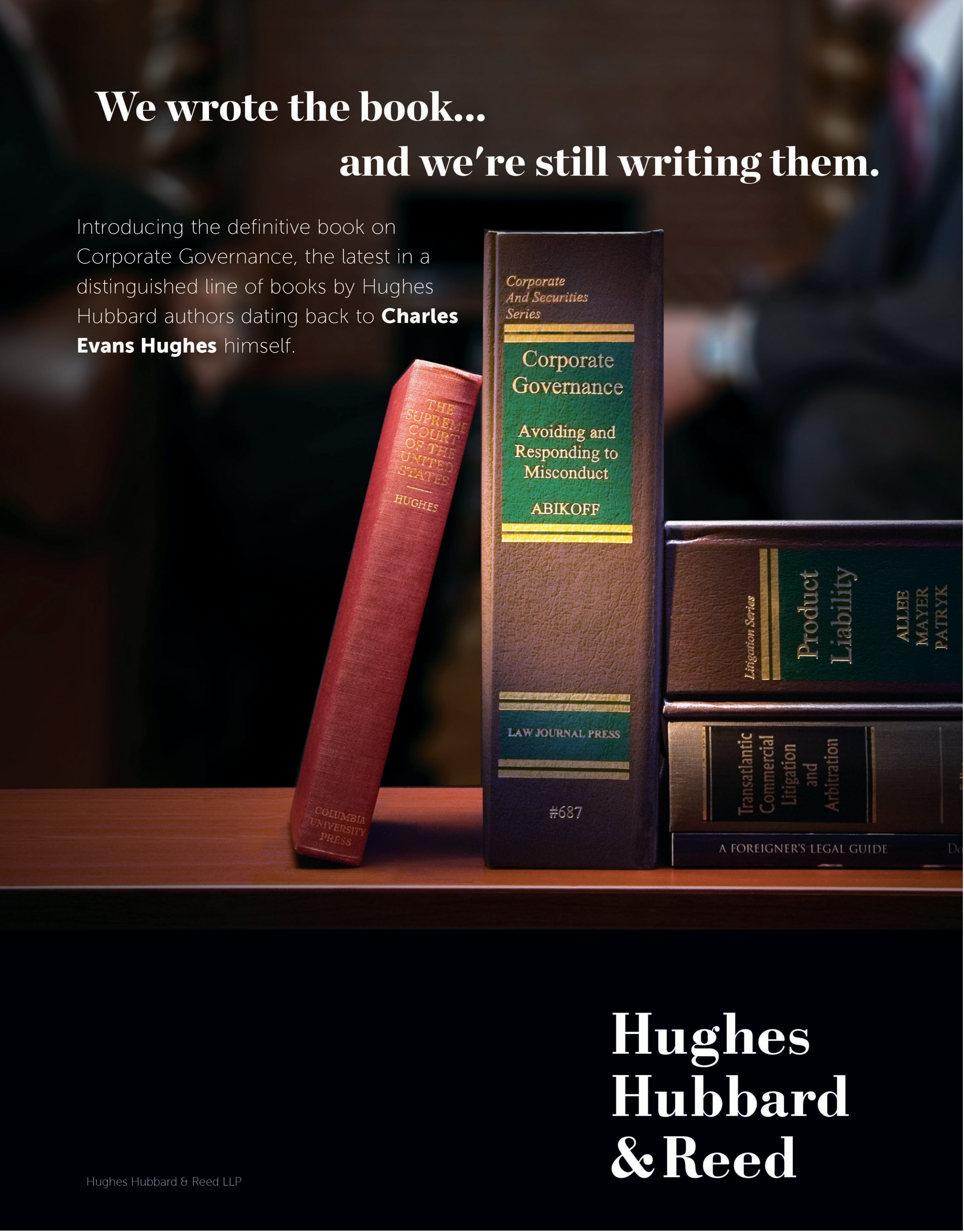
COUNSEL

Michael A. DeBernardis
Olivier Dorgans
Dina Hoffer
Alan G. Kashdan
Edward J.M. Little
John T. McGoey
Daniel J. McLaughlin
Marie-Agnès Nicolas
Sean M. Reilly
Michael R. Silverman

ASSOCIATES & INTERNATIONAL SPECIALISTS

Ayoka Akinosi
Ernesto J. Alvarado
Athena Arbes
Rayhan Asat
Nicolas Burnichon
Gil Ben-Ezra
Arnaldo Bernardi
Paul Charlot
Ana Carolina Chaves*
Marina Drapey
Jan Dunin-Wasowicz
Lucie Dzongang
Jiaxing Hao
Ashley R. Hodges
Stephen A. Fowler
Edwige Fowo
Maureen A. Howley
Clothilde Humbert
Aylin Ictemel
Adriana Ingenito
Carolyn J. Jackson
Sigrid Jernudd
Alyssa Johnson
Brian S. Kang
Robert Kolick
Tamara Kraljic
Clinton T. Lipscomb
Calvin K. Liu
Elsa Malaty
Dorsaf Matri
Megan Mollat
Lorena C. Monteiro+
Babaka Mputu
Robby Naoufal
Jessica Norrant-Eyme
Aline Rezende Peres Osorio
Miles Orton
Jordan Pate
Antonio Pimentel*
Debbie Placid
Joshua Rosenthal
Caroline Rosa*
Mathieu Rossignol
Samuel Salyer
Sergon Sancar
Yoshinori Sasao
Aleea Stanton
Jennifer Suh
Luis Gustavo Vagos*
Inès Vally
Shayda Vance
Bernardo G. Viana*
Laura Vittet-Adamson
Adam Weinstein
Mei Li Zhen
Jonathan Zygielbaum

* Saud Advogados, Rio de Janeiro, Brazil in strategic cooperation with Hughes Hubbard & Reed
+ Admission Pending


We wrote the book...
and we're still writing them.
Introducing the definitive book on Corporate Governance, the latest in a distinguished line of books by Hughes Hubbard authors dating back to **Charles Evans Hughes** himself.
THE SUPREME COURT OF THE UNITED STATES
HUGHES
COLUMBIA UNIVERSITY PRESS
Corporate And Securities Series
Corporate Governance
Avoiding and Responding to Misconduct
ABIKOFF
LAW JOURNAL PRESS
#687
Litigation Series
Product Liability
ALLEE MAYER PATRYK
Transatlantic Commercial Litigation and Arbitration
A FOREIGNER'S LEGAL GUIDE
Hughes Hubbard & Reed
Hughes Hubbard & Reed LLP

CONTRIBUTIONS

Executive Editors	***Kevin T. Abikoff*** +1 202 721-4770 kevin.abikoff@hugheshubbard.com	***Laura N. Perkins*** +1 202 721-4778 laura.perkins@hugheshubbard.com
Editorial Panel:	Benjamin S. Britz, Michael Huneke, Anne Gaustad, Bryan J. Sillaman	
Drafting Committee	Michael A. DeBernardis, Tamara Kraljic, Jonathan Zygielbaum	
Contributors	Calvin Liu, Clinton Lipscomb, Maria Mannarino, Paula Ortiz Cardona, Aline Osorio, Emma Baker, Paul Bettencourt, Win Jordan, Paula Carolyn Jackson, Brian Kang, Joshua Rosenthal, Rayhan Asat, Nicolas Burnichon, Tabitha Bartholomew, Olivier Dorgans, Edwige Fowo, Jiaxing Hao, Clothilde Humbert, Marie-Agnès Nicolas, Jessica Norrant-Eyme, Santiago Reyes Ramirez, Samuel Salyer, Sergon Sancar, Salim Saud Neto, Shayda Vance, Bernardo Viana, Laura Vittet-Adamson, Caroline Rosa, Antonio Pimentel, Ana Carolina Chaves, Luis Gustavo Vagos, Lorena C. Monteiro	

Introduction

Raise a little hell

If you want a drink of water
You got to get it from a well
If you want to get to heaven
You got to raise a little hell[1]

We are pleased to bring you our Fall 2019 FCPA & Anti-Bribery Alert. As has become tradition, we begin this Alert with a quote and theme from an entertainer we lost during the past year. The inspiration for the theme of this year's Alert is Steve Cash, who passed away in October 2019, and his band the Ozark Mountain Daredevils. Preparing this Alert, we were struck by the number of enforcement actions that described corporate failures in situations where they could or should have been stopped if more aggressive action was taken by legal or compliance personnel. The SEC's 2019 action against Barclays, for example, included an allegation that a senior Barclays compliance officer approved the hiring of the daughter of an executive of an important government customer. Despite knowing that the banker proposing the hire had referenced winning business as a reason for the hire, the compliance officer allegedly offered an "out", approving the hire as long as the candidate was hired based on her skills and qualifications. The candidate was hired and business allegedly followed. DOJ and SEC actions against Walmart offer another cautionary tale. After a construction company that Walmart's Brazilian subsidiary wanted to hire failed due diligence, the compliance department of Walmart Brazil advised the business that it could not sign any more contracts with the company. This advice was simply ignored by the business, which continued to work with the construction company in order to direct improper payments to Brazilian officials. The compliance department either couldn't or wouldn't do anything else to stop it. In both instances, it appears that compliance was in a position with a chance to "raise a little hell" and insist that the activities cease or not go forward and instead took a rather passive approach or worse.

It is important for compliance personnel to establish a good working relationship and work cooperatively with their colleagues in the business. Without this collaborative approach, compliance departments run the risk of resentment from the business and a reluctance to seek advice or guidance on important issues. However, external and internal legal and compliance advisors operating in today's environment would be wise to take note of the direction given by the Ozark Mountain Daredevils in their 1973 hit, "If you Wanna Get to Heaven:" sometimes you have to "raise a little hell."

This Alert is divided into six chapters. Chapter 1 is devoted to analysis of critical enforcement highlights, trends, and lessons from recent settlements, prosecutions, and other related developments. Following that analysis, Chapter 2 is dedicated to the U.S. FCPA and provides a description of FCPA-related charges and settlements for 2018 through publication in 2019 organized alphabetically by year. Chapter 2 also includes discussion of other relevant FCPA-related developments, including court rulings and guidance. Chapter 3 is dedicated to developments in the enforcement of the U.K. Bribery Act, including a description of recent investigations and enforcement actions of note. Chapter 4 covers an anti-corruption enforcement update from France under Loi Sapin II. Chapter 5 includes updates from other select countries: Brazil, China, and Mexico.

---

1. In honor of the late Steve Cash (1946-2019), an original member of the Ozark Mountain Daredevils and co-writer of "If You Wanna Get to Heaven." Ozark Mountain Daredevils, "If You Wanna Get to Heaven." The Ozark Mountain Daredevils (1973).

Chapter 6 provides an update related to the activities of multilateral development banks in the global fight against corruption.

For those so inclined, more information is included in our FCPA and Anti-Bribery Compendium, which is freely available on our website (www.hugheshubbard.com) and contains (i) descriptions of all FCPA settlements and criminal matters from 2005 through 2019 (including relevant updates), (ii) a summary of each DOJ Review and Opinion Procedure Release issued from 1980-present, (iii) further details and background information on the U.K. Bribery Act and multilateral development bank enforcement, and (iv) a discussion of various international developments and compliance guidance.

For more information about the matters discussed in this Alert or our Anti-Corruption and Internal Investigations practice generally, please contact us or any member of our Practice Group.

Kevin T. Abikoff
+1 202 721-4770
kevin.abikoff@hugheshubbard.com

Laura N. Perkins
+1 202 721-4778
laura.perkins@hugheshubbard.com

October 2019

Chapter 1: Highlights, Trends & Lessons

Analysis does not set out to make pathological reactions impossible, but to give the patient's ego freedom to decide one way or another.

- Sigmund Freud

I. Recent Highlights

The past year has seen several noteworthy developments in the area of anti-corruption enforcement. Below are Hughes Hubbard's "Top 10" highlights from the past twelve months. This year, in honor of the 50th anniversary of the Apollo 11 moon landing, we once again take the list to 11.

1. End of the Walmart Saga - On June 20, 2019, the seven-year investigation of Walmart Inc. ("Walmart"), an Arkansas-based retailer and the world's largest company by revenue, came to an end. In a long-awaited resolution, Walmart agreed to pay the DOJ and SEC approximately $282 million in order to settle FCPA violation charges relating to conduct by Walmart's subsidiaries in Brazil, China, India and Mexico between 2000 and 2011. Walmart entered into a three-year non-prosecution agreement ("NPA") with the DOJ and agreed to a two-year Monitorship, which is restricted in scope to select risk areas. Relatedly, Walmart's wholly-owned Brazilian subsidiary, WMT Brasilia, S.a.r.l. ("Walmart Brazil"), pleaded guilty to one count of causing a violation of the FCPA's books and records provision. As further detailed in this Alert, Walmart failed to timely implement an effective and centralized anti-corruption program. Instead, Walmart took a decentralized approach, which gave Walmart's foreign subsidiaries more freedom to design their own compliance framework and provided little oversight of the implementation of this approach. The payments made by Walmart to U.S. authorities, the Monitorship, and the reportedly $900 million paid by Walmart in legal fees, pre-resolution investigations and extensive compliance enhancements over the past seven years, should serve as effective deterrents to multinational companies considering managing compliance at their foreign subsidiaries with a lighter touch. The Walmart resolution provides a number of other substantive and procedural "lessons learned," explained in greater detail throughout this chapter.

   - Tamara Kraljic (Senior Associate), Washington, D.C.

2. French Anti-Corruption Agency's Sanctions Committee Holds First Hearing - In July 2019, the Sanctions Commission of France's new Anti-Corruption Agency ("AFA") rendered its first decision following a referral by the AFA alleging that a company (Sonepar) had failed to implement several key components of an effective compliance program. The Sanctions Commission decision provides important and much-awaited guidance for companies regarding the substantive requirements of the anti-corruption compliance program, as well as questions pertaining to procedural aspects of the AFA audits. With respect to the conduct of controls, companies should be aware of certain limits to the procedural protections afforded to companies. For example, the AFA can request documents pre-dating the entry into force of Sapin II (France's main anti-corruption law), provided such documents are "deemed relevant to the control." Moreover, the absence of minutes from the interviews of personnel conducted in the context of the control does not constitute a violation of due process rights. On the other hand, the Sanctions Commission found that the recommendations of the AFA do not have any binding legal effect. Importantly, the Sanctions Commission also indicated that the assessment of the effectiveness of the anti-corruption compliance program will be made as of the day of its public hearing (and not at the time of the AFA control), thereby leaving companies significant leeway to address and remediate potential weaknesses between the end of the AFA control and a potential Sanctions Commission hearing. On the merits, the decision should largely be viewed as a victory for Sonepar. The six independent professional judges from France's three highest courts rejected the AFA's allegation that the company had failed to implement an effective compliance program. Most prominently, the decision noted that the AFA cannot impose its recommended risk-

mapping methodology upon companies. To the extent that the risk mapping methodology is robust and conducted in good faith, it does indeed meet the requirements of the law.

- *Anne Hukkelaas Gaustad (Partner), Paris, France*

3. Deutsche Bank and the Continuing "Friends and Family" Charges - Companies might not normally consider their hiring policies as internal financial controls, but when those policies fail to prevent hires of government officials, FCPA books and records and internal controls liability may still follow. In August 2019, Deutsche Bank agreed to pay $16 million to the SEC stemming from its hiring of relatives of public officials in China and Russia. While Deutsche Bank's FCPA policy defined "anything of value" to include offers of employment as early as 2009, it did not implement a global hiring policy until 2015. In the interim, Deutsche Bank's offices in Moscow and London hired family members of Russian government officials in order to obtain business from government entities and SOEs. Meanwhile, in China, a 2010 APAC region hiring policy that specifically addressed what Deutsche Bank termed "Referral Hires" failed to stop the company from hiring numerous prohibited candidates to gain favor with Chinese SOEs. Deutsche Bank personnel evaded and overrode the policy, sometimes routing the hires through joint ventures. The SEC did not charge violations of the anti-bribery provisions of the FCPA, but instead charged that the conduct violated the books and records and internal controls provisions, a reminder that those provisions apply broadly within a company's operations, wherever corruption risk might arise.

   - *Benjamin S. Britz (Partner), Washington, D.C.*

4. Och-Ziff Restitution Ruling Adds Additional Risk to Companies Considering Plea - In 2016, Och-Ziff Capital Management Group LLC ("Och Ziff") agreed to pay more than $412 million to the DOJ and SEC to resolve allegations that it violated the FCPA and securities laws in a number of African countries. Och Ziff entered into a DPA with the DOJ, while its subsidiary, OZ Africa Management GP LLC ("OZ Africa"), pleaded guilty to conspiring to violate the anti-bribery provisions of the FCPA. Among other things, Och Ziff admitted to participating in a bribery scheme to acquire mining rights in Africa, including a copper mine in the Democratic Republic of Congo, for which exclusive rights belonged to Canadian mining company Africo Resources Ltd. ("Africo"). Before OZ Africa could be sentenced in connection with its plea agreement, Africo shareholders intervened and asked for restitution under the Mandatory Victims Restitution Act as part of any plea agreement. In September 2019, despite objections from Och Ziff and the DOJ, a federal judge in the Eastern District of New York ruled that Africo shareholders were victims under the Mandatory Restitution Act. While Judge Nicholas Garaufis has not ruled on whether the shareholders should be entitled to restitution or how much that restitution should be (Africo shareholders claimed over $1 billion in losses as a result of the corrupt scheme), the ruling could have far reaching implications. Narrowly, it could potentially upend OZ Africa's guilty plea, although it is unclear that OZ Africa could withdraw the plea at this stage even if it wanted to. More broadly, the ruling could create even more reason for companies to avoid entering into a guilty plea or subjecting even small subsidiaries to guilty pleas. Unlike DPAs and NPAs, guilty pleas require sentencing, and with that the opportunity for a victim of the bribery scheme to claim restitution.

   - *Michael A. DeBernardis (Counsel), Washington, D.C.*

5. Mobile Telesystems Resolution Puts Exclamation Point on Uzbekistan Bribery Scheme - In March 2019, Russian Mobile TeleSystems PJSC ("MTS") agreed to pay $850 million to settle charges with the DOJ and SEC, bringing to a close the third and final chapter of the U.S. and European authorities' trilogy of Uzbekistan cases. Considered with settlements by VimpelCom Limited in 2016 (more than $835 million)

and Telia Company AB in 2017 (more than $965 million), the Uzbekistan trilogy of cases resulted in more than $2.65 billion in penalties and three of the top five largest corruption-related settlements in history. At the same time, the DOJ announced charges against Ms. Gulnara Karimova, a former Uzbekistani government official and the daughter of the deceased and first President of Uzbekistan Islam Karimov, for allegedly abusing her position and influence within the Uzbekistan telecoms market to solicit and launder over $865 million in bribes from MTS, VimpelCom, and Telia. Ms. Karimova, also a pop singer who released songs under the stage name Googoosha, reportedly had a falling out with her long-ruling father in 2014, resulting in her house arrest. In 2016, the DOJ's Kleptocracy Asset Recovery Initiative seized $850 million from Ms. Karimova, and, in 2017, the U.S. Department of the Treasury sanctioned Ms. Karimova under the Global Magnitsky Human Rights Accountability Act for allegedly heading an organized crime organization that leveraged government actors to expropriate businesses, monopolize markets, solicit bribes, and extort companies. In March 2019, Ms. Karimova was transferred to a prison for violating the terms of the house arrest. It is not clear if Ms. Karimova will ever be extradited to the U.S. to face the charges against her. Nevertheless, the charges against her and MTS add an exclamation point to what was already an incredible story.

- *Calvin Liu (Senior Associate), Washington, D.C.*

6. <u>Fresenius Offers First Glimpse as to DOJ's Approach to Voluntary Disclosure of Widespread Corruption</u> - The February 25, 2019 NPA between the DOJ and Fresenius Medical Care AG & Co. KGaA ("Fresenius") provides an important data point for companies considering voluntary disclosure of expansive corrupt activity. The resolution illustrates that, in the presence of aggravating factors, the DOJ will press forward with a criminal resolution even when a company voluntarily discloses misconduct. The DOJ's Corporate Enforcement Policy establishes a presumption that the DOJ will offer a declination to companies that self-report, and that it will offer a 50% reduction off of the low end of the fine range calculated under the U.S. Sentencing Guidelines if a criminal resolution is appropriate. Despite these presumptions, Fresenius—which discovered and voluntarily disclosed that its employees had bribed public officials in a number of countries in order to obtain or maintain business for its medical products and services—was granted an NPA rather than a declination, and the associated $84.7 million fine represented a reduction of "only" 40% off the bottom end of the Sentencing Guidelines range. The DOJ did not directly address the reasons it departed from the Corporate Enforcement Policy presumptions. However, the language of the NPA indicated that the DOJ considered the seriousness of the misconduct disclosed by Fresenius, including its pervasiveness throughout an arm of the company's business and the involvement of senior executives, and that Fresenius was not fully cooperative because it did not provide timely or complete responses to certain requests. With Fresenius, the DOJ has underscored that it will treat serious misconduct with commensurate enforcement, and has provided a window into how it will view similar disclosures going forward.

- *Clinton T. Lipscomb (Senior Associate), Washington, D.C.*

7. <u>PNF-AFA Issue Guidelines on the Implementation of French Corporate Resolutions</u> - On June 29, 2019, the French Parquet National Financier ("PNF") and the AFA issued joint guidelines ("Guidelines") on the implementation of the French corporate resolution mechanism established by *Sapin II*; the Convention Judiciaire D'intérêt Public ("CJIP"). Together with a January 31, 2018 Circular by the Ministry of Justice, the Guidelines were designed to address the absence of formal guidance under the law regarding the conditions for concluding a CJIP. In practice, the Guidelines not only offer welcome clarifications regarding the availability and application of CJIPs, but they more broadly shed light upon the profound

changes to French anti-corruption enforcement policies following the adoption of Sapin II. The Guidelines define criteria that must be met for companies to be able to benefit from a CJIP, and also describes the methodology applied for the calculation of the public interest fine, associated anti-corruption compliance program requirements, coordination with foreign authorities and the AFA's role in overseeing compliance with the French blocking statute. Most prominently, the Guidelines condition the availability of a CJIP on timely voluntary disclosure, cooperation and past instances of misconduct by the company and/or its subsidiaries and senior executives, which clearly echoes U.S. enforcement practices and policies but maintains the specificities of the French CJIP regime. While the Guidelines constitute a welcome development to provide companies with a solid overview of how prosecutors will likely approach a CJIP negotiation, companies should be aware of potential areas of concern with respect to confidentiality and legal privilege considerations. In particular, the Guidelines take a skeptical view of the applicability and importance of protections afforded by legal privilege and indicate that the level of the company's cooperation may be adversely affected by the refusal to transmit documents on the basis of legal privilege. Additionally, documents provided as part of the criminal investigation stage, do not, in the view of the PNF and the AFA, benefit from appropriate confidentiality guarantees, which would likely disincentivize companies to self-disclose. More broadly, the Guidelines demonstrate deep changes to the French anti-corruption enforcement regime, where the prosecution services are equipped with more flexible and effective enforcement tools, and where companies are expressly encouraged to adopt a cooperative approach with the prosecution services and the AFA.

- Bryan J. Sillaman (Partner), Paris, France

8. <u>CFTC Enters Foreign Bribery Fight</u> - Anti-corruption enforcement was once almost entirely the domain of the U.S. DOJ and SEC. Over the past several years, anti-corruption enforcement has spread across the globe, with new legislation and regulators appearing around every corner. This year another new face – and not one many would have expected – hopped aboard the enforcement train. On March 6, 2019, the Division of Enforcement of the U.S. Commodity Futures Trading Commission (CFTC) issued an Enforcement Advisory on Self-Reporting and Cooperation for Commodities Exchange Act Violations Involving Foreign Corrupt Practices (the "Advisory"). CFTC's Enforcement Director, James McDonald, concurrently announced the Advisory in his remarks at the American Bar Association's 33rd National Institute on White Collar Crimes. The announcement sent out clear signals that the CFTC will investigate foreign bribery schemes as violations, not of the FCPA, but of the Commodities Exchange Act (CEA).

   - Michael A. DeBernardis (Counsel), Washington, D.C.

9. <u>DOJ Offers New Compliance Guidance</u> - On April 30, 2019, the DOJ published a guidance document on the "Evaluation of Corporate Compliance Programs," designed to be used by U.S. prosecutors when evaluating companies' compliance programs. While this document is substantively similar to previously issued guidance that has existed in some form since 2004, a close review of the April 2019 guidance offers insight into topics currently emphasized by the DOJ. In particular, the guidance identifies regular Risk Assessments as an essential tool for properly designing, implementing, and evaluating an effective compliance program, and reveals the DOJ's increasing focus on whether companies appropriately collect, analyze, and utilize measurable data regarding their compliance program.

   - Samuel Salyer (Senior Associate), Washington, D.C.

10. <u>TechnipFMC Resolution Breaks New Ground in Brazil</u> - In June 2019, TechnipFMC reached the first global settlement negotiated with the U.S. DOJ and, at the same time, the Brazilian Federal Public

Prosecutors' Office (MPF), the Office of the Comptroller General (CGU) and the office if the Attorney General of Brazil (AGU). The settlement was the first time the three agencies jointly resolved a case with the U.S. authorities, placing the CGU and the AGU in the forefront of the international cooperation on anticorruption enforcement in Brazil, in a place previously taken almost exclusively by the MPF.

- Salim Saud (Partner Saud Advogados), Rio de Janeiro, Brazil

11. Quad/Graphics Demonstrates Need for Quick and Effective Compliance Changes After M&A - On September 26, 2019, the SEC announced that Quad/Graphics Inc. ("Quad"), a publicly listed, Wisconsin-based digital and print marketing provider, had agreed to pay nearly $10 million to resolve charges that it violated the FCPA's anti-bribery, books and records, and internal controls provisions by engaging in multiple bribery schemes in Peru and China. The Quad case highlights the FCPA pitfalls for companies in an M&A context; more specifically for companies which, through acquisitions, expand their operations from domestic only to international sales but fail to adjust their compliance program accordingly. Until 2010, Quad's sales were focused on the U.S. domestic market and Quad's compliance program was, according to the SEC, "almost non-existent". That year, Quad acquired a Canadian company with an extensive international portfolio. Rather than anticipating this increase in international presence and thereby its augmented risk profile, calling for a need for greater compliance controls, Quad did not appoint its first Director of Compliance until 2011 (i.e. one year after the 2010 acquisition) and only first rolled out broad anti-corruption compliance training for employees in 2012 (i.e. two years after the acquisition). The SEC's order implies that had Quad stepped up its compliance program to reflect the increased risk flowing from the international operations, much of the alleged misconduct – which took place between 2011 and 2016 and was orchestrated by foreign subsidiaries – could have been prevented or detected earlier.

- Tamara Kraljic (Senior Associate), Washington, D.C.

II. Trends & Lessons

The combination of resolved actions, ongoing criminal and regulatory investigations, guidance issued by regulatory authorities, and other developments discussed below underscore a number of important themes of which companies should be aware in conducting their operations, designing and implementing their compliance programs, considering whether to enter into potential transactions or to affiliate with an international agent, intermediary, or joint venture partner, and dealing with government agencies. These themes take the form of both enforcement trends and practice lessons.

A. Trends

- *International Coordination:* The DOJ and SEC continue to rely upon and provide assistance to a growing number of non-U.S. enforcement agencies in complex bribery investigations. The DOJ credited authorities from the following countries for assistance in its FCPA prosecutions in 2019 and 2018: Austria, Bahamas, Belgium, Brazil, Cayman Islands, Croatia, Cyprus, France, Germany, India, Ireland, Isle of Man, Italy, Latvia, Luxembourg, Malta, Mexico, the Netherlands, Norway, Singapore, Spain, South Africa, Sweden, Switzerland, Turkey, and the United Kingdom.

- *U.S. Law Enforcement Cooperation*: In addition to cooperation with foreign agencies, the DOJ and SEC credited a wide variety of domestic agencies and divisions for their assistance in various of its investigations in 2018 and 2019: (i) FBI, (ii) IRS Criminal Investigation,

(iii) ICE Homeland Security Investigations, (iv) U.S. Postal Inspection Services, (v) the Federal Reserve Bank of New York, (vi) Department of Energy Office of Inspector General, and (vii) the CFTC. It is clear that U.S. prosecutors have vast and varied resources available to investigate foreign bribery allegations.

- *Tailored Monitorships?*: Walmart's resolution of FCPA charges was interesting for a number of reasons, including the structure of its monitorship. In addition to the fact that Walmart's monitor reportedly began work approximately six months prior to its DOJ and SEC settlements, the Walmart monitorship is limited to Walmart's compliance controls in certain key risk areas (including real estate transactions and licensing and permitting) in four countries. As such, Walmart appears to be an application of DOJ guidance issued on October 11, 2018 on the Selection of Monitors in Criminal Division Matters (authored by Assistant Attorney General Brian Benczkowski). The so-called "Benczkowski Memo" clearly states that "the scope of any monitorship should be appropriately tailored to address the specific issues and concerns that created the need for the monitor."

- *SEC's Broad View of Accounting Provisions:* The SEC has firmly taken the position that the "books and records" provisions apply to all kinds of records generated by the company, whether related to financial reporting or not. For example, the SEC claimed that misrepresentations by Deutsche Bank employees in internal forms regarding the source of referral hires (i.e., failing to indicate that the candidate was referred by a public official) constituted a books and records violation. The SEC has also invoked the accounting provisions related to transactions that have no relation to corruption. For example, the SEC charged Quad/Graphics with violating the FCPA's books and records provisions for concealing prohibited sales in Cuba.

- *Other Third Party Risks:* For years, regulators, practitioners, and compliance professionals have been warning of the corruption risks associated with sales agents and consultants. The use of these third parties was, and continues to be, a favorite source for corrupt actors to disguise their illicit actions. However, enforcement over the past two years demonstrates the real risks associated with other types of third parties, such as distributors, sub-distributors, and joint venture partners.. For example, the SEC's 2019 cease and desist order against Juniper Networks details Juniper Networks' alleged use of excessive discounts to resellers to create slush funds through which bribes could be paid. In connection with the 2019 Stryker settlement, the SEC noted at least 21 sub-distributors (operating under one state-owned "hub"-distributor) sold Stryker's products in China without going through any type of review, approval, or training by Stryker China. In connection with its NPA with Fresenius in 2019, the DOJ highlighted Fresenius' use of distributors and joint ventures, among other things, as a means to conceal corrupt activity. Westport Fuels' 2019 settlement with the SEC also alleged use of a joint venture relationship to funnel payments to Chinese government officials.

- *Focus on Tech*: Historically, tech companies have not been watched as closely for FCPA violations as, for example, oil and pharmaceutical companies, whose industries have been subject to FCPA enforcement "industry sweeps". However, Microsoft's 2019 FCPA settlement with the DOJ and SEC may be indicative of a new FCPA enforcement focus. Juniper Networks, a California-based technology company, resolved its own FCPA issues in August 2019. Open FCPA investigations involving tech companies of note include the investigation of ride-sharing company Uber Technologies, first reported by the Wall Street Journal in August 2017.

- *Focus on Banks and Financial Services*: Following on the heels of the high-profile FCPA settlements with Och-Ziff in 2016, Société Générale and Credit Suisse in 2018, large banks and bankers continue

to be targets of FCPA-related investigations. In 2019, both Deutsche Bank and Barclays resolved allegations that they violated the FCPA through their hiring practices, primarily in the Asia Pacific region. Meanwhile, Goldman Sachs has disclosed that the bank itself is under investigation for the actions of its employees in connection with the 1MDB scandal. Moreover, bankers and financial advisors are increasingly finding themselves ensnared in FCPA prosecutions. Tim Leissner (Goldman Sachs), Frank Chatburn (financial advisor based in Miami) and Andrew Pearse, Surjan Singh, and Detelina Subeva (Credit Suisse) have been prosecuted for their roles in massive fraud and corruption cases in Malyasia, Ecuador and Mozambique, respectively. As banks continue to explore opportunities in the developing world, the exposure to FCPA risks will only increase.

- *Prosecution of Foreign Government Officials:* We noted in last year's Alert that prosecutors seemed to be actively looking for ways to charge foreign government officials involved in corrupt schemes. Although such officials are not covered under the FCPA (which prohibits only active bribery), the trend of using money laundering, and wire fraud and securities fraud laws to prosecute foreign government officials has continued. The prosecutions of Manuel Chang (p. 38), Antonio do Rosario (p. 38), Teofilo Nhangumele (p. 38), Master Halbert (p. 33), and Gulnara Karimova (p. 36), among others, are prime examples of this continued effort.

- *Focus on High-Risk Jurisdictions*: Not surprisingly, the conduct that led to the various enforcement actions over the past two years was largely concentrated in countries with a known history of pervasive corruption. Among the most prevalent, China featured in 15 enforcement actions in 2018 and 2019 and Brazil in 13 enforcement actions.

- *Emphasis on Timely Remediation:* The DOJ and SEC have long signaled that extensive cooperation with their investigations and full remediation may result in less severe penalties. Past enforcement has demonstrated that the DOJ and SEC expect cooperation to be timely and will offer less credit to companies who delay in cooperating. Enforcement in 2018 demonstrated that the DOJ and SEC also consider timely remediation to be of paramount importance. In its April 2018 DPA with Panasonic, the DOJ afforded Panasonic "only" 20% off of the low end of the U.S. Sentencing Guideline range rather than the 25% for which Panasonic was otherwise eligible. Given that the DOJ credited Panasonic's cooperation and remedial measures, it is reasonable to assume that Panasonic was docked 5% as a result of its "delayed" remedial measures.

B. Lessons from Recent Enforcement Activity

- *Application of Corporate Enforcement Policy*: Recent enforcement action and declination decisions provide some important data points regarding how the Corporate Enforcement Policy is being applied by the DOJ when companies voluntarily report FCPA violations. For example, with Fresenius's 2019 settlement, we now have an example of how the DOJ may treat a company that discloses widespread and serious corruption (as opposed to the smaller, more isolated corruption common in most of the initial declination decisions). Despite the fact that Fresenius voluntarily reported misconduct, cooperated with the investigation, and took remedial measures, the DOJ did not decline to prosecute. Rather, the DOJ agreed "only" to a reduction of 40% off of the low end of the U.S. Sentencing Guidelines Fine Range, apparently due to the nature and seriousness of the offense and certain delays in cooperation. In other instances, however, it remains unclear exactly how the DOJ arrived at the decision to decline to prosecute. For example, the DOJ declined to prosecute Cognizant, despite the fact that Cognizant's President and Chief Legal Officer were involved in or aware of the illicit conduct. As a justification for this decision, the DOJ cited the existence and effectiveness of

Cognizant's preexisting compliance program. However, the SEC charged Cognizant with failing to devise and maintain sufficient internal accounting controls and found that the company "failed to adequately enforce its corporate antibribery and anticorruption policies." Finally, the requirement that companies pay disgorgement in order to be eligible for treatment under the Corporate Enforcement Policy continues to be as vexing as predicted. For the most part, when companies have entered parallel resolutions with the SEC in which the companies agree to pay disgorgement, the DOJ has credited that disgorgement in connection with the declination decision. The Polycom resolution indicates that may not always be the case. Despite agreeing to pay the SEC $16 million in disgorgement, the DOJ required Polycom to pay $10 million more in disgorgement to obtain a declination related to the same charges. While questions may persist, with each declination decision, companies are presented additional data points to inform a potential decision whether to voluntarily disclose an FCPA violation.

- *Companies Moving into International Business Must Adopt Compliance Programs*: It is by now well understood that companies should take a risk-based approach to anti-corruption compliance programs. Companies with largely domestic business are often justified in investing relatively fewer resources in controls regarding foreign corruption. However, as business operations change (whether organically or through acquisition), so must compliance programs. The Quad 2019 settlement with the SEC highlights this point. As specifically highlighted in the SEC's order, Quad's sales were focused on the U.S. domestic market until 2010, when Quad acquired the Canadian printing company, World Color Press, which had a large international portfolio. As the acquisition substantially increased Quad's international presence, it also increased the company's compliance risk profile. However, as pointed out by the SEC, Quad's compliance program was "almost non-existent in 2010". Among other things, the SEC noted that the company appointed its first Director of Compliance in 2011, one year after the 2010 acquisition, and even then, hired "an individual with no compliance experience or training and [only] and information technology background." Although not stated in these direct terms, the SEC's order implies that had Quad stepped up its compliance program to reflect the increased risk flowing from the international operations acquired from World Color Press, much of the alleged misconduct – which took place between 2011 and 2016 and was orchestrated by former World Color Press subsidiaries – could have been prevented or detected earlier. Moreover, the SEC's order highlights how new compliance measures must be accompanied with a genuine change of the compliance culture. The SEC noted, for example, that when Quad first rolled out its anti-corruption compliance training for employees in 2012 (two years after the World Color Press acquisition), senior U.S.-based executives for Latin America failed to support these efforts, jokingly alluding to the lucrative bribery scheme in Quad's Peruvian subsidiary.

- *Adequately and Appropriately Investigate and Respond to Allegations*: Enforcement agencies expect companies to adequately and appropriately investigate allegations or evidence of misconduct. In order to take advantage of the benefits of the Corporate Enforcement Policy announced in 2017 and updated in 2019, which sets forth a presumption that the DOJ will decline to prosecute companies which voluntarily self-disclose, cooperate fully and remediate in a timely and appropriate fashion, companies must understand the nature of potential misconduct as quickly as possible and, in any event, prior to the news reaching the DOJ.

- *Adequately responding to allegations includes properly staffing investigations*: For instance, in its 2019 settlement with Walmart, the DOJ noted that following a whistleblower report in 2005 regarding serious allegations of corruption, Walmart tasked its internal audit department with investigating the matter. When the initial findings of the internal audit department suggested violations of the law,

Walmart appointed a senior lawyer within Walmart Mexico to look into the matter, despite the fact that the lawyer himself had been named in the whistleblower report.

- *Need for Appropriate Due Diligence and Monitoring of Business Partners*: The vital importance of risk-based due diligence of third parties is one of the most important lessons to guide the development and implementation of an effective corporate compliance program. The DOJ's 2019 memorandum on "Evaluation of Corporate Compliance Programs" explicitly states that the DOJ will look at whether the company has in place risk-based controls for engaging and monitoring third-parties. This focus on the importance of effective risk-based due diligence has also been embraced by the international community. OECD guidance on internal controls, ethics, and compliance programs counsels towards the adoption of a risk-based approach to due diligence. The World Bank Integrity Compliance Guidelines and African Development Bank Integrity Compliance Guidelines also require that companies have in place a process for risk-based due diligence on all third parties.

  The importance of due diligence on third parties has also been borne out in recent enforcement actions. Seventeen of the 26 U.S. corporate settlements and prosecutions in 2018 and 2019 involved third-party agents or intermediaries. In almost every one of those cases, the DOJ or SEC criticized the companies for failing to conduct appropriate due diligence on their third-party agents or intermediaries, or for ignoring red flags that suggested that there was a high probability that the payments to such entities would be passed on to government officials. For example, in describing Microsoft's internal controls failures in Hungary, the SEC highlighted that Microsoft's Hungarian subsidiaries entered into agreements with third parties without conducting any due diligence.

  - *Determine Identities of Beneficial Owners:* Shell companies and other similar entities can easily be used to conceal the identities and locations of their beneficial owners, and thus the true source or destination of funds. Any due diligence procedure must seek to learn the identities of all beneficial owners and actual control persons of shell companies, holding companies, and trusts that maintain an ownership interest in an agent or third party.

  - *Examine Carefully the Qualifications of Agents, Distributors, and other Third Parties:* Companies must understand the background and qualifications of agents and intermediaries. The SEC criticized Kinross Gold (*see* p. 58) for example, for awarding a $50 million logistical support contract to a less-qualified shipping company with ties to a Mauritanian government official, rather than to a more qualified and cheaper competitor.

  - *Examine Carefully Tasks to be Performed by Third Parties:* Companies must examine the specific tasks that a third party will perform, and the justification for retaining the third party to perform those tasks. Companies should also validate the tasks allegedly being provided by the third party. In 2018 and 2019, enforcement actions against Fresenius, Microsoft, Quad, Elbit Imaging Ltd., Kinross Gold, Panasonic Avionics Corporation, and PDVSA suppliers Rincon & Shiera all involved third parties paid through agreements for nonexistent services.

  - *Ensure that Compensation is Commensurate with Services*: Once validating the services provided by the third party, companies must ensure that the compensation is commensurate with those services. Even with no other risk factors, excessive compensation can be a significant red flag, particularly in high risk jurisdictions.

- *Dangers in Decentralized Approach to Compliance:* Many companies have adopted a decentralized approach to their anti-corruption compliance programs, relying on divisions, regions, countries, or subsidiaries to implement tailored compliance programs within broader principles and frameworks dictated by headquarters. This approach has several benefits, allowing the compliance program more flexibility to adjust to unique cultural differences throughout the organization and to be tailored to the specific risks facing each element of the business. However, Walmart's "Freedom within a Framework" approach also demonstrates the dangers in such an approach. Certain Walmart locations simply did a poor job of implementing an effective compliance program, or did a poor job of executing the compliance programs that had been implemented. With little oversight from headquarters, subsidiaries in various locations around the world separately ended up with materially deficient compliance controls. Walmart's resolution highlights the need and importance of regular and thorough auditing and monitoring of decentralized compliance programs and of ensuring a common ground of clearly-defined "base" compliance standards, to be applied at a minimum by all global subsidiaries.

- *Compliance Programs and Internal Controls Must be Effective at Preventing Misconduct:* Year after year, enforcement actions illustrate that simply maintaining a compliance program is not enough. Compliance programs and internal controls must be adequate and effective at preventing and detecting misconduct. Recent enforcement actions have reflected a willingness by the SEC to pursue FCPA claims even when companies have established compliance programs at the time of the misconduct and the employees involved intentionally evaded the controls in place. In 2018, for example, the SEC found that Panasonic had failed to maintain adequate internal controls because, among other things, the company's employees were able to evade third-party due diligence requirements. The SEC noted that Panasonic's due diligence procedures were ineffective because employees were able to engage sales agents as subagents of a third party that had successfully completed the due diligence process. According to the SEC, Panasonic employees were able to direct payments to 13 uncertified third parties through one agent that had successfully completed the due diligence process. In a more recent example, Deutsche Bank, established a policy and related procedure specific for its APAC region regarding referral hiring. Deutsche Bank employees allegedly ignored or otherwise bypassed these controls to continue hiring relatives of government officials and other customers.

  These enforcement actions underscore the importance to companies of continuously testing and reviewing their compliance programs to ensure that they are adequately designed to prevent misconduct.

- *Holistic Approach to Compliance Improvements:* In describing Walmart's failings with respect to its Chinese subsidiary, the DOJ pointed in particular to at least one Walmart U.S. executive who had learned of the earlier allegations in Mexico. This suggests that the DOJ expects companies to take a proactive approach to ensure that issues discovered in one location are not occurring in others. Indeed, it appears companies are expected to take a holistic and global approach to compliance, and cannot hide behind geographic or functional siloes to justify inaction.

- *Conduct Effective M&A Due Diligence*: Pre-acquisition or post-acquisition anti-corruption due diligence is now a regular part of most corporate acquisitions. The pressure to ensure that such due diligence is effective in identifying potential misconduct is as high as ever. Several recent corporate resolutions involved the use of corporate transactions to conceal illicit payments (*see,* e.g., MTS and Fresenius).

- *Structure and Staff Compliance Functions Appropriately*: Government regulators have emphasized the need for companies to take measures to ensure that their compliance obligations are taken seriously at the highest level of management and that the compliance function is appropriately structured, staffed, and funded. The SEC, for example, criticized Quad/Graphics for appointing as its Director of Compliance an individual without any prior compliance experience.

- *Apply Close Scrutiny to High Risk Subsidiaries or Units*: High risk subsidiaries, business units, joint ventures, and other operations must be carefully and closely monitored. Regulators have been clear that compliance resources should be properly apportioned to high-risk areas of the business. The April 2018 SEC enforcement action against Dun & Bradstreet, for example, was based on the actions of two Dun & Bradstreet subsidiaries in China. One of Dun & Bradstreet's subsidiaries formed a joint venture with a local firm, but even after learning that this local firm had used its government connections to source non-public and restricted information from government agencies, Dun & Bradstreet failed to adopt controls that could prevent such behavior. Instead, Dun & Bradstreet merely provided a short FCPA training to executives of the joint venture partner and required the joint venture to source the necessary information through third parties rather than through existing government connections. Dun & Bradstreet also acquired another company in China that purchased data from third-party vendors. Although Dun & Bradstreet uncovered significant red flags during its pre-acquisition due diligence on this local entity, the Company failed to follow up on these red flags after the acquisition. Dun & Bradstreet's settlement demonstrates the need for companies to closely scrutinize the activities of high-risk subsidiaries, and to implement compliance controls that adequately address the risks presented by such operations.

- *Importance of De-confliction*: De-confliction, the practice of a company waiting to interview a witness until after the prosecutors have had an opportunity to do so, has received increased attention in recent years as the DOJ has specifically tied the practice to the amount of cooperation credit a company can receive. The 2017 Corporate Enforcement Policy specifically lists de-confliction as a prerequisite to receiving full cooperation credit (and thus creating eligibility for a declination). In April 2019, the DOJ revised the Corporate Enforcement Policy to, among other things, make it clear that the de-confliction requirement was not meant as a means for prosecutors to manage internal investigations and would only be required where requested and "appropriate." Walmart's resolution with the DOJ provides a prime example of how the failure to de-conflict (among other things) can result in reduced cooperation credit. In Walmart's NPA, the DOJ noted that Walmart received full credit for its cooperation in Brazil, China and India, but only partial credit for its cooperation in Mexico (the splitting of cooperation credit by territory is also a novel approach). With respect to Mexico, the DOJ noted that Walmart did not timely provide documents in response to certain requests and failed to de-conflict with respect to one witness as requested by the DOJ. As a result, for the portion of the penalty attributable to conduct in Mexico, Walmart received a 20% reduction, compared to the 25% attributable to the conduct in Brazil, China, and India.

III. By the Numbers

Facts, figures, and statistics that reflect anti-corruption enforcement over the past 12 months:

850 million

Amount, in dollars, that MTS agreed to pay to resolve DOJ and SEC investigations into corrupt payments MTS made in Uzbekistan, marking it the third largest calculated FCPA penalty ever (behind Odebrecht's $2.6 billion penalty in 2016 and Petrobras's $853 million penalty in 2018).

10.15 million	*Additional* amount, in dollars, that the DOJ required Polycom to disgorge (beyond the approximately $16 million Polycom agreed to pay in disgorgement to the SEC) in connection with the DOJ's decision to decline to prosecute Polycom under the Corporate Enforcement Policy related to corrupt conduct by Polycom in China.
4	Number of major financial institutions that have now resolved FCPA charges related to hiring sons and daughters of government officials in Asia Pacific (with the addition of two in 2019: Deutsche Bank and Barclays).
14	Number of corporations to resolve FCPA charges with the SEC since the release of Hughes Hubbard's 2018 FCPA and Anti-Bribery Alert.
5	Number of federal trials in October 2019 for FCPA violations or fraud or money laundering charges related to foreign bribery, an unprecedented number for the prosecutors in the DOJ's FCPA Unit.
39	Number of individuals prosecuted by the DOJ for FCPA-related violations in the past year.
25	Number of corporate FPCA resolutions since the beginning of 2018, out of 47 total, that involved conduct in China or Brazil.
17	Number of Chinese companies debarred by the World Bank for corrupt or fraudulent conduct in 2019, a 340% increase from 2018.

Chapter 2: FCPA

The Department's white-collar prosecutions and resolutions should send an unmistakable message to the private sector: We are serious about fighting corporate fraud and corruption, and we are serious about doing so through resolutions that are fair and effective.

- Brian Benczkowski, 33rd Annual ABA National Institute on White Collar Crime Conference, March 8, 2019

I. FCPA Elements and Penalties

The FCPA has two fundamental components: (1) the Anti-Bribery Provisions in Section 30A of the Securities Exchange Act of 1934 ("Exchange Act")[2] and in Title 15, United States Code,[3] and (2) the Books and Records and Internal Accounting Control Provisions in Sections 13(b)(2)(A)[4] and 13(b)(2)(B)[5] of the Exchange Act, respectively (collectively, the "Accounting Provisions"). The DOJ has exclusive jurisdiction to prosecute criminal violations of the FCPA, while the DOJ and the SEC share jurisdiction over civil enforcement actions.

A. Anti-Bribery Provisions

The FCPA's Anti-Bribery Provisions prohibit: (i) an act in furtherance of (ii) a payment, offer or promise of, (iii) anything of value, (iv) to a foreign official,[6] or any other person while knowing that such person will provide all or part of the thing of value to a foreign official, (v) with corrupt intent, (vi) for the purpose of either (a) influencing an official act or decision, (b) inducing a person to do or omit an act in violation of his official duty, (c) inducing a foreign official to use his influence with a foreign government to affect or influence any government decision or action, or (d) securing an improper advantage, (vii) to assist in obtaining or retaining business.[7]

The term "foreign official" is broadly defined to mean any officer or employee of a foreign government, agency or instrumentality thereof, or of a public international organization, or any person acting in an official capacity on behalf of such government, department, agency, or instrumentality, or public international organization.[8] The term foreign official has been construed by federal prosecutors to include employees, even relatively low-level employees, of state-owned institutions.

Under the FCPA, "a person's state of mind is 'knowing' with respect to conduct, a circumstance, or result" if he or she has actual knowledge of the conduct, circumstance or result or "a firm belief that such circumstance exists or that such result is substantially certain to occur."[9] In addition, knowledge of a circumstance can be found when there is a "high probability" of the existence of such circumstance.[10] According to the legislative history,

> [T]he Conferees agreed that "simple negligence" or "mere foolishness" should not be the basis for liability. However, the Conferees also agreed that the so called "head-in-the-sand" problem—variously described in the pertinent authorities as "conscious disregard," "willful blindness" or "deliberate ignorance"—should be covered so that management officials could not take refuge from the Act's prohibitions by their unwarranted obliviousness to any action (or inaction), language or other "signaling [*sic*] device" that should reasonably alert them of the "high probability" of an FCPA violation.[11]

2. Codified at 15 U.S.C. §§ 78dd-1(a).
3. 15 U.S.C. §§ 78dd-2(a), 78dd-3(a).
4. Codified at 15 U.S.C. § 78m(b)(2)(A).
5. Codified at 15 U.S.C. § 78m(b)(2)(B).
6. The FCPA further prohibits payments to foreign political parties and officials thereof.
7. *See* 15 U.S.C. §§ 78dd-1(a).
8. 15 U.S.C. §§ 78dd-1(f)(1).
9. *Id.*
10. *See* 15 U.S.C. § 78dd-1(f)(2)(B).
11. H.R. Rep. No. 100-576, at 920 (1987) (Conf. Rep.), *reprinted in* 1988 U.S.C.C.A.N. 1547, 1953.

Since the 1977 enactment of the FCPA, the Anti-Bribery Provisions have applied to U.S. and foreign issuers of securities that registered their securities with or reported to the SEC and to domestic concerns such as U.S. citizens and companies organized under U.S. law or with a principal place of business in the United States, if the U.S. mails or a means or instrumentalities of U.S. interstate commerce (such as an interstate wire transfer) were used in furtherance of the anti-bribery violation.[12] In 1998, amendments to the Anti-Bribery Provisions generally extended U.S. jurisdiction to cover acts outside of U.S. territory in furtherance of an anti-bribery violation by U.S. issuers and domestic concerns and acts inside U.S. territory in furtherance of an anti-bribery violation by other persons, such as foreign non-issuers and foreign nationals, who were not previously subject to the FCPA.[13] Such extended jurisdiction is not dependent upon the use of U.S. mails or means or instrumentalities of U.S. interstate commerce.[14]

The FCPA also applies to officers, directors, employees, or agents of any organization subject to the FCPA and to stockholders acting on behalf of any such organization.[15]

B. The Exception and Defenses to Alleged Anti-Bribery Violations

Under the FCPA, facilitating payments "to expedite or to secure the performance of a routine governmental action" are excepted from the Anti-Bribery Provisions.[16] This is a narrow exception, only applying to non-discretionary acts such as obtaining official documents or securing utility service and not applying to any decision to award or continue business with a particular party.[17] Also, its practical effect is limited because many other jurisdictions and international conventions do not permit facilitation payments.

There are two affirmative defenses to an FCPA charge. Under the "written law" defense, it is an affirmative defense to an FCPA prosecution if the payment, gift, offer, or promise of anything of value that is at issue was lawful under the written laws and regulations of the recipient's country.[18] It is also an affirmative defense if the payment, gift, offer, or promise of anything of value was a reasonable, *bona fide* expenditure directly related either to the promotion, demonstration, or explanation of products or services, or to the execution or performance of a contract with a foreign government or agency.[19] Both defenses, however, are narrow in practice and, because they are affirmative defenses, it would be the defendant's burden to prove their applicability in the face of an FCPA prosecution.

C. Accounting Provisions

The FCPA's Accounting Provisions apply to issuers who have securities registered with the SEC or who file reports with the SEC.[20] The Books and Records Provisions compel such issuers to make and keep books,

---

12. 15 U.S.C. §§ 78dd-1(a), 78dd-2(a).
13. 15 U.S.C. §§ 78dd-1(g), 78dd-2(i), 78dd-3(a).
14. *Id.*
15. 15 U.S.C. §§ 78dd-1(a), (g), 78dd-2(a), (i), 78dd-3(a).
16. 15 U.S.C. §§ 78dd-1(b), 78dd-2(b), 78dd-3(b).
17. 15 U.S.C. §§ 78dd-1(f)(3)(B), 78dd-2(h)(4)(B), 78dd-3(f)(4)(B).
18. 15 U.S.C. §§ 78dd-1(c)(1), 78dd-2(c)(1), 78dd-3(c)(1).
19. 15 U.S.C. §§ 78dd-1(c)(2), 78dd-2(c)(2), 78dd-3(c)(2).
20. 15 U.S.C. § 78m(b)(2). The Accounting Provisions were passed as part of the original 1977 FCPA legislation out of concern over companies improperly recording payments on their books and records and failing to fully account for illicit "slush" funds, from which improper payments could be made. These provisions, however, have broader application than simply within the context of the FCPA. For purposes of this Alert, when violations of these provisions are alleged in the context of improper payments to foreign officials or similar conduct, they are referred to as violations of the FCPA's Accounting Provisions. When violations occur in situations not involving improper payments (*see,* e.g., the Willbros Group

records and accounts which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer.[21] The Internal Accounting Controls Provisions require such issuers to devise and maintain a system of internal accounting controls regarding accounting for assets, enabling the preparation of financial statements, and providing reasonable assurances that management authorizes transactions and controls access to assets.[22] As used in the Accounting Provisions, "reasonable detail" and "reasonable assurances" mean a level of detail and degree of assurance as would satisfy prudent officials in the conduct of their own affairs.[23]

D. Penalties

The FCPA imposes both criminal and civil penalties. Willful violations of the Anti-Bribery Provisions carry maximum criminal fines of $2 million for organizations and $250,000 for individuals, per violation.[24] Under U.S. criminal law, alternative fines of up to twice the pecuniary gain from the offense apply instead, if the alternative fine exceeds the maximum fine under the FCPA.[25] Individuals also face up to five years' imprisonment for willful violations of the Anti-Bribery violations.[26] Anti-bribery violations also carry civil penalties of up to $16,000 for organizations or individuals, per violation.[27] These fines may not be paid by a person's employer or principal.[28]

Willful violations of the Accounting Provisions carry maximum criminal fines of $25 million for organizations and $5 million for individuals, or, if greater, the alternative fine of twice the pecuniary gain.[29] Individuals face up to 20 years' imprisonment for willful violations of the Accounting Provisions.[30] Civil penalties for violations of the Accounting Provisions include disgorgement of any ill-gotten gains and penalties up to $775,000 for organizations and $160,000 for individuals, per violation, in actions brought by the SEC.[31]

II. Tracking Policy Changes

A. Evaluation of Compliance Programs

On April 30, 2019, the Department of Justice's Criminal Division published updated guidance for prosecutors regarding the assessment and evaluation of corporate compliance programs.[32] The Evaluation of Corporate Compliance Programs (the "April 2019 Guidance") modifies guidance that has existed in some form since the adoption of the amended U.S. Federal Sentencing Guidelines in 2004, and was last revised in February of 2017. The April 2019 Guidance is meant to assist prosecutors to determine the appropriate form of resolution, a suitable monetary penalty, and any additional compliance obligations contained in a resolution.

---

settlement discussed *infra*), they are described as the Exchange Act's books and records and/or internal controls provisions.

21. 15 U.S.C. § 78m(b)(2)(A).
22. 15 U.S.C. § 78m(b)(2)(B).
23. 15 U.S.C. § 78m(b)(7).
24. 15 U.S.C. §§ 78ff(c), 78dd-2(g), 78dd-3(e); 18 U.S.C. § 3571(b)(3), (e) (fine provision that supersedes FCPA-specific fine provisions).
25. 18 U.S.C. § 3571(d), (e) (fine provision that supersedes FCPA-specific fine provisions).
26. 15 U.S.C. §§ 78ff(c)(2)(A), 78dd-2(g)(2)(A), 78dd-3(e)(2)(A).
27. 15 U.S.C. §§ 78ff(c), 78dd-2(g), 78dd-3(e); *see* DOJ & SEC, A RESOURCE GUIDE TO THE FOREIGN CORRUPT PRACTICES ACT (2012) (indicating that the maximum civil penalty for an anti-bribery provision violation is $16,000, but citing the SEC's announcement of the adjustment for issuers subject to SEC enforcement without citing to a parallel DOJ announcement for domestic concerns and other persons).
28. 15 U.S.C. §§ 78ff(c)(3), 78dd-2(g)(3), 78dd-3(e)(3).
29. 15 U.S.C. § 78ff(a); 18 U.S.C. § 3571(d), (e).
30. 15 U.S.C. § 78ff(a).
31. 15 U.S.C. § 78u(d)(3), (5); *see* 17 C.F.R. § 201.1005, Table V (2013) (adjusting the amounts for inflation).
32. Available at https://www.justice.gov/criminal-fraud/page/file/937501/download.

Much of the guidance is substantively similar to prior editions, but whereas the February 2017 Guidance discussed 46 compliance program elements organized under 11 specific themes (e.g., Policies and Procedures, Autonomy and Resources, Training and Communications), the April 2019 Guidance re-organizes the elements around three questions: (1) whether the company's compliance program is well-designed; (2) whether the compliance program is effectively implemented; and (3) whether the compliance program works in practice.

1. Is the compliance program well-designed?

In analyzing whether a program is well-designed, the DOJ will look at whether the program can accurately identify risks specific to the company's business and location. Indeed, it positions risk assessments as a central means by which companies are expected to create, monitor, and improve their compliance practices. A company's risk assessment should be designed "to detect the particular types of misconduct most likely to occur in a particular corporation's line of business." These risk assessments should be "tailor made" and "periodically updated."

The DOJ will also look at what policies and procedures the company has in place, and whether those policies and procedures have been made accessible to employees. Similarly, the DOJ will assess compliance training programs to directors, officers, employees, and third parties. The April 2019 Guidance instructs prosecutors to evaluate, among other factors, (i) the guidance and training provided to employees with approval authority or certification responsibilities, (ii) whether supervisory employees have received specialized or supplementary compliance training, (iii) whether employees are evaluated on their compliance knowledge to assure a minimum level of competency, (iv) the turnover rate among and the seniority of compliance function personnel, and (v) whether concerns voiced by compliance personnel are adequately considered. The April 2019 Guidance notes the importance of a company's collection, tracking, maintenance, and analysis of compliance-related data points, such as incident response times, reports of misconduct, and due diligence results. The April 2019 Guidance emphasizes a company's duty to promptly investigate and address allegations of misconduct arise. The DOJ will also look into third-party due diligence and M&A pre-acquisition due diligence to ensure the due diligence process includes controls and monitoring related to the qualifications and type of work being provided.

2. Is the compliance program being implemented effectively?

When determining if a compliance program is being implemented effectively, the DOJ will look to see if the program is merely a "paper program" or one that is "implemented, reviewed, and revised, as appropriate, in an effective manner." Effective implementation requires commitment by senior and middle management to promote and oversee the compliance program. The April 2019 Guidance makes clear that the DOJ expects corporate compliance functions to be staffed by personnel with sufficient qualifications, experience, and training to understand and identify potential risks to the company. Prosecutors are also instructed to analyze whether the company has outsourced all or part of its compliance function to outside counsel, the qualifications of such outside counsel, and the level of access granted to outside counsel. Companies should provide both positive and negative incentives to ensure compliance by its employees. This includes providing bonuses for specific actions such as improving or developing compliance programs or demonstrating ethical leadership, tying promotions to compliance, including compliance as a metric for compensation, and publicizing disciplinary actions imposed on employees involved in misconduct.

3. Is the compliance program working in practice?

According to the April 2019 Guidance, the DOJ will consider how the company has reviewed, evaluated, and revised its compliance program in light of its experiences and instances of misconduct. The DOJ acknowledges that the existence of misconduct does not, by itself, mean that a compliance program is ineffective. The DOJ will

assess the effectiveness and promptness of the company's internal investigations. The DOJ will also look at whether the company conducts root-cause analyses of misconduct to identify how misconduct occurred and prevent future incidents. A company should conduct periodic testing and internal audits to reveal areas of risk and potential adjustment.

Running through the April 2019 Guidance is a focus by the DOJ on the collection, tracking, maintenance, and analysis of compliance-related data points, such as incident response times, reports of misconduct, and results of due diligence. Prosecutors are instructed to evaluate how companies have analyzed such data to find patterns of misconduct, locate signs of compliance weaknesses, and develop metrics that can be used to evaluate compliance processes.

B. Changes to Corporate Enforcement Policy

In March 2019, the DOJ announced changes to the FCPA Corporate Enforcement Policy (initially adopted in November 2017). While the basic framework of the Corporate Enforcement Policy remains untouched, the most significant changes include:

- Messaging Applications – One of the most controversial aspects of the Corporate Enforcement Policy was the requirement that, in order to obtain full cooperation credit, companies had to prohibit the use of communication applications that do not retain records or the communications. In effect, the Corporate Enforcement Policy targeted instant messaging programs that did not automatically retain messages and third party messaging apps such as WhatsApp and WeChat. The updated Corporate Enforcement Policy no longer includes a strict prohibition on such communication methods. Rather, companies are required to implement appropriate policies and controls regarding the use of these programs to ensure that business records are properly retained.

- De-Confliction – The original Corporate Enforcement Policy indicated that companies had to de-conflict (coordinate interviews of relevant individuals with the DOJ), leading to criticism that the DOJ would or could exercise control over a company's internal investigation. In effect, the concern from the legal community was that companies and their counsel would need to confer with the DOJ prior to each interview. The updated Corporate Enforcement Policy addresses this concern by limiting the de-confliction requirement to circumstances where it is "appropriate" and including a footnote directly indicating that the DOJ will not be taking steps to "direct a company's internal investigation efforts."

- Application to M&A – In 2018, Deputy Assistant Attorney General Matthew Miner hinted that the DOJ would apply the same criteria from the Corporate Enforcement Policy to circumstances where a successor company voluntarily disclosed a violation of its predecessor company when pre-acquisition due diligence is not possible. The update to the Corporate Enforcement Policy formalized this approach. The Corporate Enforcement Policy also states that acquiring companies with established and robust compliance programs are especially likely to receive a declination if they voluntarily disclose the misconduct.

- Providing Information regarding Responsible Employees – The updated Corporate Enforcement Policy also formalizes a clarification announced by then-Deputy Attorney General Rod Rosenstein that full cooperation credit does not require companies to disclose information regarding all employees involved in the corrupt conduct. Rather, companies must disclose all relevant facts known regarding all individuals "substantially involved in or responsible for" the corrupt conduct.

C. Inability to Pay

On October 8, 2019, Assistant Attorney General Brian Benczkowski issued a memorandum regarding "Evaluating a Business Organization's Inability to Pay a Criminal Fine or Criminal Monetary Penalty."[33] As the title suggests, the memo was written to guide prosecutors when considering an argument from a business organization that it is unable to pay a criminal fine or monetary penalty.

As a threshold matter, AAG Benczkowski confirmed that the burden of establishing an inability to pay rests on the organization asserting such a claim. As such, it is incumbent on the organization to provide a complete and timely response to the Inability-to-Pay Questionnaire (included as an attachment to the memo) and provide any additional information and documentation as may be requested. Where the Inability-to-Pay Questionnaire raises legitimate concerns regarding the organizations ability to pay, the memo explains that prosecutors will consider a range of factors, including:

- Context for Organization's Financial Condition – What caused the inability to pay? Did the management take capital out of the organization in the form of bonuses, dividends or other means? Has the organization fallen on hard times or recently made investments in capital improvements or an acquisition?

- Alternative Sources of Funds – What alternative sources of funds can the organization draw from? Does the organization have access to new credit facilities? Can it sell assets? According to the memo, Criminal Division attorneys should also consider the existence of insurance and indemnification agreements, plans for divestments of assets, and company forecasts for future performance.

- Collateral Consequences –Will the criminal fine or monetary penalty have collateral consequences? Will it affect the organization's ability to fund pension obligations or maintain the level of maintenance, capital or equipment required by law? Is it likely to cause layoffs? Is it likely to affect the market, including disrupting competition?

- Victim Restitution – Will the proposed fine or monetary penalty prevent the organization from paying restitution to victims?

When Criminal Division attorneys conclude that an organization is unable to pay the proposed fine or monetary penalty, the memo directs them to recommend an adjusted amount, reduced only to the extent necessary to avoid threatening the continued viability of the organization or avoid impairing the ability of the organization to pay restitution to victims. The memo indicates that, in addition to reductions, Criminal Division attorneys should consider a payment plan to facilitate the payment of the fine or penalty within a reasonable time period.

33. Available at https://www.justice.gov/opa/speech/file/1207576/download.

III. FCPA Settlements and Enforcement Actions[34]

A. 2019[35]

1. 1MDB Prosecutions

Key Facts:

Agencies: DOJ
Countries Involved: Malaysia, China, U.S., Abu Dhabi
Means of Corruption: Cash, gifts, travel, homes
Notes: In addition to pleas from Goldman bankers, the DOJ has charged Low and is reportedly investigating Goldman itself. Former Malaysian Prime Minister Razak is being prosecuted in Malaysia.

Over the last several years, authorities in the U.S., Malaysia, Switzerland, and elsewhere have uncovered a globe-spanning scheme to pilfer assets from 1Malaysia Development Berhad (“1MDB”), a sovereign wealth fund created in 2008 ostensibly to pursue investment and development projects to benefit Malaysia and its people. Enforcement authorities have alleged that billions of dollars were misappropriated from the fund by public officials and their co-conspirators. Beginning in early 2016, the DOJ has pursued civil forfeiture actions under the Kleptocracy Asset Recovery Initiative aimed at recovering assets pilfered from 1MDB (discussed in Section III).

On November 1, 2018, the DOJ unsealed money laundering and FCPA-related charges against Low Taek Jho, more commonly known as Jho Low, and Ng Chong Hwa, also known as Roger Ng. Mr. Low, a Malaysian national who, although never formally employed by 1MDB, is accused of being the central figure in the scheme to plunder the sovereign wealth fund. Mr. Ng served as Managing Director of several subsidiaries of Goldman Sachs (“Goldman”), which underwrote more than $6 billion in bonds issued by 1MDB from 2012-2013. Low and Ng are charged with conspiring to launder money embezzled from 1MDB, conspiring to violate the FCPA by paying bribes to various Malaysian and Abu Dhabi officials, and, in Ng’s case, conspiring to circumvent Goldman’s internal accounting controls.

On the same day, the DOJ also unsealed the guilty plea of Tim Leissner, the former Southeast Asia Chairman of Goldman and the participating managing director responsible for Goldman’s relationship with 1MDB. Leissner, a German national, pleaded guilty to charges of conspiracy to launder money and conspiracy to violate the FCPA by paying bribes to various Malaysian and Abu Dhabi officials and circumventing Goldman’s internal accounting controls.

According to court filings, between approximately 2009 and 2014, Low and his co-conspirators misappropriated and diverted $2.7 billion from 1MDB. Low used the funds for his own personal benefit and to pay millions of dollars in bribes and kickbacks to government officials in Malaysia (including then-Prime Minister Najib Razak and his family members) and Abu Dhabi. Previous DOJ asset recovery actions have outlined how Low and others laundered these funds by purchasing real estate, jewelry, artwork, a $250 million yacht, and even financed Hollywood films such as *Wolf of Wall Street*. 1MDB raised much of its funds through three bond offerings underwritten by Goldman that took place in 2012 and 2013. According to the allegations, Low and his co-

34. Hughes Hubbard represents or has represented multiple companies that have been the subject of the enforcement actions or other activities summarized in this Alert. All details and information provided in this Alert in connection with such enforcement actions, however, are based solely on the government’s charging documents or other publicly available documents. Additionally, all descriptions of allegations underlying the settlements (or other matters such as ongoing criminal cases) discussed in this Alert are not intended to endorse or confirm those allegations, particularly to the extent that they relate to other, non-settling entities or individuals.
35. Cases and settlements have been organized alphabetically within each year.

conspirators worked with Goldman to raise billions of dollars through these bond offerings, and then almost immediately diverted the funds to shell companies that they personally controlled.

As early as 2009, Leissner and Ng, among others, attempted to introduce Low as a Goldman private banking client, believing that he would be able to deliver lucrative business deals to Goldman. Goldman's Compliance Group and Intelligence Group, however, refused to approve Low as a client citing, in part, concerns about his source of wealth. Despite this, Leissner, Ng, and other's within Goldman continued to work with Low in connection with 1MDB and ultimately hid his involvement in the 1MDB bond offerings from Goldman's Compliance and Intelligence staff.

According to court documents, in 2012, 1MDB selected Goldman as the sole arranger for a $1.75 billion debt financing transaction that was guaranteed by the International Petroleum Investment Company, the sovereign wealth fund of Abu Dhabi. In order to obtain approvals for this guarantee, Leissner, Ng and Low, along with other co-conspirators, arranged to pay bribes to government officials in Abu Dhabi. The three also arranged to pay bribes to Malaysian government officials in order to receive their approval to move forward with the bond offering. In May 2012, when the offering closed, approximately $577 million of the bond proceeds were misappropriated and directed to a bank account held by a shell company that was controlled by Low. These funds were distributed to accounts controlled by Low, his associates, government officials, or their relatives.

The “Project Maximus” and “Project Catalyze” bond offerings followed similar patterns. The offerings purported to raise more than $4 billion for 1MDB's investment and development projects. Instead, Low and his associates allegedly diverted an additional nearly $2 billion into bank accounts controlled by Low, or by government officials in Malaysia and Abu Dhabi. In total, Goldman earned nearly $600 million in fees and revenues from these transactions. Leissner and Ng personally received millions of dollars in bonuses in connection with these transactions.

While Low remains at large, Ng was arrested in Malaysia, where he also faces criminal charges. On May 6, 2019, after Malaysian authorities reached an agreement to transfer Ng to the U.S. to face trial, Ng appeared in the Eastern District of New York and pleaded not guilty to all charges.

As part of his guilty plea, Leissner, who is also facing charges in Malaysia, agreed to forfeit $43.7 million. He is scheduled to be sentenced December 17, 2019, and is reportedly cooperating with U.S. authorities.

2. Barclays

Key Facts:

Agencies: SEC
Amount of Total Financial Settlement: $6.3M
Countries Involved: China, Korea
Means of Corruption: Hiring

On September 27, 2019, Barclays PLC ("Barclays") consented to an administrative cease and desist order in connection with SEC allegations that Barclays violated the internal accounting controls and recordkeeping provisions of the FCPA. Barclays agreed to pay approximately $6.3 million in civil penalty and disgorgement to the SEC.

Barclays is a London-based bank holding company. From 2009 to 2013, Barclays' subsidiaries in Seoul and Hong Kong provided valuable employment opportunities to the friends and relatives of government officials and executives of Barclays' non-government clients. According to the SEC, Barclay's referral hiring program began in Korea in 2009, when Barclays Korea started an "unofficial intern" program to provide work experience opportunities for Korean students and provide opportunities for "relationship" hires. These relationship hires were designed to enhance business relationships and hiring decisions included the importance of the client that was referring the candidate. This practice, which began in Korea, expanded to other areas of Asia Pacific ("APAC").

In September 2010, Barclays APAC bankers allegedly sought to hire the daughter of a senior executive of a Chinese state-owned entity. The SEC alleged that the candidate performed poorly during the hiring process, receiving a "do not hire" recommendation. Nevertheless, the relationship banker pressed to make her an offer, noting that her familial relationship would likely bring financial benefits to Barclays. The SEC alleged that a senior Barclays compliance officer approved the transaction knowing that the responsible banker had referenced winning business as a reason for her hire. The compliance officer apparently approved the hire as long as the candidate was hired based on her skills and qualifications.

In May 2011, Barclays APAC established a procedure to manage the risks and processes associated with relationship hires. The procedure ultimately included compliance approval requirements for relationship hires. Despite the implementation of this program, bankers in APAC allegedly continued to make relationship hires in violation of Barclays stated anti-corruption policy. According to the SEC, Barclays personnel simply ignored the procedure or provided false or incomplete information regarding the purpose of the hire when the opportunity was significant enough. For example, the SEC alleged that when a Korean banker indicated that a customer had guaranteed business if Barclays could find his daughter a job, a senior banker in Korea falsified the candidate's approval application, failing to disclose her relationship with the customer (a Korean bank). Two months after retaining the candidate, Barclays priced $500 million in senior binds for the Korean bank, earning over $300,000 in fees in the process.

In March 2012, Barclays attempted to strengthen its controls around referral hires. In particular, Barclays added a requirement that employees attest that a particular referral hire was not being made to obtain or retain business. Although this requirement was implemented in APAC, the SEC alleged that personnel in APAC either offered inaccurate attestations or compliance approved the hire despite the connection to business opportunities.

In January 2013, Barclays global compliance department took steps to address the risks associated with relationship hiring. Among other things, the global compliance department issued specific guidance on Employee Referrals, which reaffirmed that employees were prohibited from hiring relationship candidates in an effort to obtain or retain business. Regardless, the SEC alleged that APAC bankers continued to send candidates for processing based on their connections to individuals that could provide business to Barclays. For example, the

SEC highlighted an incident in March 2013, just two months following the global compliance guidance on the subject. The nephew of the CEO of a key private client was allegedly offered a summer internship despite the fact that he had previously been rejected during the merit-based competition. The SEC alleged that there was no indication that the compliance department was consulted on the offer. In May 2013, Barclays earned over $2.5 million in revenue from the private client.

According to the SEC, from 2009 to 2013, Barclays hired at least 117 candidates referred by or connected to foreign government officials or non-government clients.

The SEC pointed to several compliance failures within Barclays that allowed this practice to begin and continue. Despite having a global anti-corruption policy explicitly addressing anti-corruption risks associated with hiring as early as 2009, many personnel were allegedly unaware of the policy or the specific provisions. By April 2009, Barclays compliance officers in APAC were aware of the internship program. However, compliance officers allegedly only reviewed these internships for potential conflicts of interest, with some compliance officers indicating that they were unaware of the policy addressing the anti-corruption risks associated with hiring. Moreover, the SEC detailed several instances of APAC personnel evading the compliance controls that were in place. According to the SEC, many internship decisions were simply made without consulting the compliance department or by withholding critical information from the compliance department. As a result, the SEC concluded that Barclays failed to devise and maintain a sufficient system of internal controls. Moreover, as a result of inaccurate candidate questionnaires and attestation forms completed by APAC personnel, the SEC concluded that Barclays violated the books and records provisions of the FCPA.

In September 2013, on the heels of news reports regarding investigations into the hiring practices at financial institutions, Barclays again tightened its controls around hiring. According to the SEC, Barclays took significant steps to strengthen its controls, including by adopting a specific “Anti-bribery & Corruption Employment & Work Opportunity Standards,” providing targeted training, and adopting independent testing and monitoring over hiring.

In its settlement with the SEC, Barclays agreed to pay $3.82 million in disgorgement, $1.5 million in civil penalties, and $984,000 in prejudgment interest, without admitting or denying any wrongdoing. The SEC credited Barclays for voluntarily disclosing the misconduct, taking remedial action (including terminating senior executives and other employees involved), and cooperating with the SEC’s investigation.

3. Cognizant

Key Facts:

Agencies: SEC
Amount of Total Financial Settlement: $25 million
Countries Involved: India
Means of Corruption: Third-party contractor

On February 14, 2019, the DOJ obtained an indictment against two former high-ranking executives of Cognizant Technology Solutions (“Cognizant”), Gordon Coburn and Steven Schwartz, on charges related to a scheme to bribe Indian officials in order to obtain construction permits. The DOJ declined to prosecute Cognizant, a publicly traded Fortune 200 technology services company based in the United States with extensive operations in India.

Both Coburn, Cognizant’s former President, and Schwartz, the former Chief Legal Officer, were charged with conspiracy to violate the FCPA, violations of the FCPA’s anti-bribery provision, and books and records and internal controls violations.

On February 15, 2019, the SEC filed a cease and desist order against Cognizant, and announced that the company had agreed to pay a total of $25 million, including approximately $19 million in disgorgement and

interest and a penalty of $6 million, to settle charges that Cognizant violated the anti-bribery, books and records, and internal accounting controls provisions of the FCPA. The SEC also filed civil charges against Coburn and Schwartz, seeking permanent injunctions, monetary penalties, and officer-and-director bars against the former executives.

a. The Chennai Bribery Scheme

According to the indictment, the scheme began in 2014 when Cognizant executives bribed an Indian official to obtain a planning permit. At the time, Cognizant had spent years constructing a 17,000 employee office complex in Chennai without the requisite permit. Both the DOJ and the SEC observed that this was not unusual: in fact, most Indian construction projects began without the required pre-construction permitting. After Cognizant requested a planning permit in early 2013, one Indian government agency conditionally approved the permit in late 2013 pending an order from another government agency. By early 2014, nearly a year later, that other Indian agency had yet to issue its order.

In April 2014, Coburn and Schwartz allegedly authorized a $2 million bribe in order to obtain the order that Cognizant required. They allegedly tasked an employee of Cognizant India to carry out the bribery scheme, which involved routing the bribe through Cognizant's construction contractor. For its role, the contractor would allegedly be reimbursed the $2 million it paid on Cognizant's behalf, along with a $500,000 commission. The DOJ alleged that the scheme intended that the reimbursement and commission would be disguised through a series of previously-rejected change orders that totaled approximately $2.5 million.

To ensure that Cognizant's construction contractor followed through with the scheme, Coburn allegedly pressured the contractor by directing subordinates to freeze and withhold payments to the contractor, and warned the contractor that its future business with Cognizant was in jeopardy. In response, the contractor said that it would take the necessary steps to carry out the scheme, and allegedly hired a third party to make the bribe. In May 2014, Coburn received confirmation that the contractor was moving ahead with the plan, causing Coburn to partially release withheld funds while keeping the remainder until the contractor completed its task. In June 2014, the contractor secured the government order, and Coburn allegedly again partially released withheld funds while withholding the remainder. In November 2014, Indian authorities issued the planning permit, at which point Coburn allegedly released the remaining funds to the construction contractor.

In late 2014, Cognizant's construction contractor began submitting a series of change order requests related to the office construction project. As agreed with Coburn and Schwartz, one claim included a $2.5 million request for "Statutory approvals – planning permit." Cognizant allegedly replaced this request with 11 previously rejected claims worth approximately the same amount, and a Cognizant employee allegedly directed a co-conspirator to create a fake claims list, falsify invoices, and create supporting spreadsheets, so that the contractor would receive payment without documenting the true purpose of the reimbursement. Cognizant's Indian subsidiary then issued payments to the construction contractor between 2015 and 2016.

The DOJ also alleged that, beginning in 2014, Coburn and Schwartz furthered their scheme by began making false representations and omissions on their certifications and annual reports, as well as by circumventing internal controls regarding payments and approvals for accounts payable.

b. Other Bribery Schemes in India

While the DOJ indictment was limited to one bribery scheme in Chennai, the SEC charges detail several other bribery schemes in India. The SEC alleged that in 2013 Cognizant India authorized a contractor to pay a

$770,000 bribe to obtain environmental clearance for a construction project in Pune, and reimbursed the contractor through a series of change order requests in 2014. In another scheme that began in 2012, Cognizant India allegedly authorized a contractor to pay $840,000 in various bribes for construction-related permits for a project in Siruseri. Between 2015 and 2016, Cognizant India reimbursed the contractor using change order requests. Finally, in a third scheme between 2013 and 2016, Cognizant India allegedly paid $27,000 in bribes for operating licenses at six Indian facilities, which were disguised in Cognizant India's records using generic descriptions like "liaison," "consulting," and "miscellaneous."

The SEC also charged Coburn and Schwartz with violating the FCPA's anti-bribery, books and records, and internal accounting controls provisions, and with aiding and abetting Cognizant's violations of these provisions. The SEC is seeking civil monetary penalties, as well as permanent bars on Coburn and Schwartz from serving as an officer or director of a publically traded company.

A third Cognizant executive, former COO Sridhar Thiruvengadam, settled SEC charges in September 2019. The Administrative Order issued by the SEC states that Thiruvengadam was aware of and did not object to the bribery scheme, and that he helped conceal the scheme by providing false management representations to Cognizant's auditors. The SEC Order notes that Thiruvengadam has agreed to cooperate with the SEC's investigation and to pay a civil penalty of $50,000.

c. DOJ Declination

Although Cognizant's President and Chief Legal Officer were directly involved in the scheme to bribe Indian officials, the DOJ declined to prosecute the company itself. Instead, in a February 13, 2019 letter made available on the DOJ website, the DOJ announced that it had declined to prosecute Cognizant based on an assessment of the factors set forth in DOJ's Principles of Prosecution of Business Organizations and its Corporate Enforcement Policy. The DOJ identified ten different factors in favor of declination, including Cognizant's timely and voluntary self-disclosure, the company's history of good behavior and proactive efforts to remediate and improve its compliance program, and the nature of the offense.

4. Deutsche Bank AG

Key Facts:

Agencies: SEC
Amount of Total Financial Settlement: $16 million
Countries Involved: China, Russia, Other Asia
Means of Corruption: Hiring

On August 22, 2019, Deutsche Bank AG ("Deutsche Bank") consented to the entry of a cease and desist order and agreed to pay more than $16 million as part of a settlement with the SEC relating to violations of the internal controls and books and records provisions of the FCPA. According to the SEC, Deutsche Bank failed to devise and maintain a system of internal controls around its hiring practices that were sufficient to provide reasonable assurances that employees did not use internships and other forms of employment as a means to bribe foreign government officials. From at least 2006 through 2014, Deutsche Bank provided employment to the relatives of foreign government officials in both the Asia-Pacific region and Russia as a personal benefit to the officials in order to improperly influence them to assist the bank in obtaining or retaining business or other benefits. Without admitting or denying the allegations, Deutsche Bank agreed to pay disgorgement of $10,785,900, prejudgment interest of $2,392,950 and a $3 million civil penalty.

According to the SEC, from at least 2006, Deutsche Bank's Asia-Pacific ("APAC") operations provided employment or internships to relatives of executives of state-owned entities ("SOEs") that were either clients or

prospective clients. Client referral hires were known at Deutsche Bank as “Referral Hires” or “Relationship Hires” and were designed specifically to generate business for Deutsche Bank. The SEC alleged that when bankers submitted a client referral request, Deutsche Bank management in APAC inquired as to what role the referral’s parent performed to determine whether the referral hire could lead to business for Deutsche Bank, even asking for a quantification of the fees that could be generated as a result of the hire.

The SEC alleged that Referral Hires were not required to compete with other candidates in Deutsche Bank’s standard merit-based hiring process. Referral Hires allegedly had no formal application process or minimum standards in terms of educational record. According to the SEC, Deutsche Bank APAC employees even took steps on occasion to help Referral Hires look more qualified, altering their resumes and providing interview questions in advance.

In 2010, Deutsche Bank enacted a written hiring policy specifically for the APAC region to detect and prevent corrupt hiring practices. Among other things, Deutsche Bank created a questionnaire that bankers were required to complete when seeking approval for a Referral Hire. The questionnaire solicited information regarding the source of the referral and whether the Referral Hire was related to any government officials. Completed questionnaires were supposed to be submitted to human resources and the compliance department for review. According to the SEC, this hiring policy was not effectively enforced.

Senior Deutsche Bank employees in APAC allegedly ignored or deliberately bypassed the hiring policy by directing Deutsche Bank’s China-based joint venture to hire prohibited candidates and evade the policy. Moreover, the SEC alleged that managers in APAC exploited a gap in the hiring policy, which did not apply to “lateral” hires. As a result, after a candidate was hired by the China-based JV, APAC managers could hire the candidate to Deutsche Bank as a lateral hire without being subjected to compliance review.

The cease and desist order provides several examples of the Referral Hire process in place at Deutsche Bank and how Deutsche Bank evaded controls to use the process to generate business. For example, the SEC alleged that executives from a Chinese SOE referred a candidate to Deutsche Bank who was the daughter of the Chairman of the SOE. Deutsche Bank could not hire the candidate directly due to the hiring policy in place and her limited credentials. As a result, management in APAC directed the China-based joint venture to retain the candidate and give her “VIP” treatment. The joint venture retained the candidate despite records indicating that she failed the admissions tests and performed poorly during interviews. After a few months, the candidate was seconded to Deutsche Bank and eventually hired as an employee of Deutsche Bank. During this time period, Deutsche Bank carried out two transactions for the SOE, earning at least $3.75 million.

According to the SEC, Deutsche Bank’s internal controls around the hiring process were insufficient, resulting in a violation of the internal controls provision of the FCPA. The SEC also concluded that employees created false books and records that concealed corrupt hiring practices. Employees allegedly knowingly submitted false and inaccurate documentation in connection with the Referral Hires, misrepresenting the identity of the referral, falsely claiming that government officials were not the referral source, and concealing the purpose of the hire. These acts, according to the SEC, resulted in a violation of the books and records provision of the FCPA.

In agreeing to resolve the matter, the SEC considered Deutsche Bank’s remedial action and cooperation with the investigation. Deutsche Bank cooperated by regularly sharing facts of its internal investigation, producing documents, identifying issues and facts that would be of interest to the SEC’s staff, and providing key documents and factual chronologies to the SEC. The SEC also credited Deutsche Bank’s remedial actions, which included enhancing its internal controls and its anti-corruption compliance program and hiring practices on a global basis, requiring that its anti-corruption office review and approve each hire of a candidate referred by a client, potential

client, or government official, instituting procedures and practices to monitor and audit Referral Hires, and increasing anti-bribery training that specifically addresses hiring practices.

5. Fresenius Medical Care

Key Facts:

Agencies: DOJ and SEC
Amount of Total Financial Settlement: $231.7 million
Countries Involved: Angola, Saudi Arabia, Morocco, Spain, Turkey, China, Serbia, Bosnia, Mexico, Other West Africa
Means of Corruption: M&A; procurement; third party consultants and distributors; joint ventures

On February 25, 2019, Fresenius Medical Care AG & Co. KGaA ("Fresenius") admitted that it violated the FCPA's internal controls and anti-bribery provisions and agreed to pay a monetary penalty of approximately $84.7 million under a three-year non-prosecution agreement (NPA) with the DOJ. The SEC separately settled a related matter with Fresenius, in which the company agreed to pay an additional $147 million in disgorgement. The settlements also subject Fresenius to a two-year period of review by an independent compliance monitor.

Fresenius is a German company that provides medical products and services for patients with chronic kidney failure, operating more than 3,700 dialysis clinics worldwide. During the relevant time period, Fresenius' American Depositary Receipts were traded on the New York Stock Exchange, making Fresenius an "issuer" under the FCPA.

Fresenius admitted to paying bribes to public officials in various countries to obtain or maintain business for its medical products and services. In addition, Fresenius admitted to knowingly and willfully failing to implement reasonable internal accounting controls and maintain books and records that accurately reflected its transactions in numerous countries. The conduct incurred in Angola, Saudi Arabia, Morocco, Spain, Turkey, China, Serbia, Bosnia, Mexico, and several countries in West Africa. The following summary provides a sample of Fresenius' admitted FCPA violations.

a. Relevant Violations

i. Angola

Between 2010 and 2014, Fresenius offered and paid bribes to an Angolan military health officer, members of his family, and to prominent nephrologists employed by the Angolan government. As part of this scheme, Fresenius offered a 15% interest in its local subsidiary to the Angolan military health officer, another 15% to two publicly employed nephrologists, and 5% to NefroAngola, a local company owned exclusively by Angolan nephrologists. These minority shareholders never paid for their shares. Fresenius retained several publicly employed nephrologists as consultants, paying monthly consulting fees ranging from €2,500 to €5,000, even though these doctors never provided any services to Fresenius. Fresenius also awarded storage contracts worth $1.48 million to a company owned by the Angolan military health officer's sons, even though none of Fresenius' products were ever stored at the facility. Fresenius paid only $560,000 of these contracts. The remaining amount was not paid due to the initiation of Fresenius' internal investigation. Fresenius garnered estimated proceeds of $12.6 million from its improper payments in Angola.

ii. Saudi Arabia

Between 2007 and 2012, Fresenius offered and paid bribes to publicly employed doctors and other officials to expand its market share in Saudi Arabia. The relevant doctors and officials were employees of a Saudi medical organization and a governmental charity. To circumvent accounting controls, Fresenius' Saudi distributor engaged

in a fraudulent check-cashing scheme. The distributor issued checks to its employees and then directed the employees to cash the checks and return the cash to the general manager of the distributor. The general manager then used the cash to pay Saudi doctors and other public officials. The general manager falsely recorded these checks as "project marketing expenses" or "collection commissions" in the distributor's financial statements, which were ultimately consolidated with Fresenius' financial statements. Fresenius channeled approximately $1.7 million to Saudi doctors and other public officials through this scheme. The same distributor also made improper payments to government doctors and officials using sham consulting and commission agreements for which no services were provided. In addition, the distributor provided expensive gifts and luxury travel to Saudi government doctors, nurses, and their family members. The distributor also made improper payments to Saudi customs officials to expedite customs processing for Fresenius products. Once the internal investigation began in 2012, the general manager of the Saudi distributor ordered employees to destroy or alter company documents and lie to investigators.

During the relevant time period, Fresenius garnered profits of approximately $42.7 million from its improper payments in Saudi Arabia.

iii. Morocco

From approximately 2006 to 2010, Fresenius offered and paid bribes to a Moroccan nephrologist charged with executing contracts to create dialysis centers at Moroccan military hospitals. Specifically, Fresenius channeled 10% of the total value of each contract to the nephrologist in exchange for winning the bid to develop dialysis centers at two Moroccan military hospitals. Fresenius falsely recorded the improper payments to the nephrologist as "commissions." This scheme resulted in $3.7 million in proceeds.

iv. Spain

Between 2007 and 2014, Fresenius used fictitious consulting agreements to retain several publicly employed doctors or professionals to receive advance information about public tenders in Spain. Fresenius also provided gifts and other benefits—such as travel and charitable donations—to the public officials to gain an improper advantage in the dialysis market. Many of these payments were falsely recorded as consulting expenses. Fresenius earned approximately $23.8 million from its improper payments in Spain.

v. Turkey

Between 2005 and 2014, Fresenius bribed publicly employed nephrologists in Turkey. In exchange, the nephrologists directed patients from their public hospitals to Fresenius' Turkish clinics. Fresenius entered into various joint ventures with two Turkish nephrologists who held minority stakes (between 20% and 35%) in these joint ventures, then repurchased the nephrologists' shares at a price calculated based on the number of patients referred by each nephrologist. The two nephrologists never paid for their original shares, yet generated profits of $451,000 and $356,000 respectively from Fresenius' purchase of their shares. Fresenius earned approximately $1.3 million from this scheme.

vi. West Africa

Fresenius' West African operations include business in Benin, Burkina Faso, Cameroon, Chad, Gabon, Ivory Coast, Niger, and Senegal. Between 2007 and 2016, Fresenius paid bribes to publicly employed health officials in several of these countries. In Gabon, Benin, Burkina Faso, Senegal, Ivory Coast, and Niger, Fresenius entered into agreements with officials of state-owned hospitals, under which Fresenius would pay kickbacks to the officials

for each kit of Fresenius' dialysis products sold at these hospitals. Fresenius also entered into service agreements with third-party companies, under which Fresenius paid "daily fees" for purported services in West Africa. These fees were channeled to public officials in Gabon and Cameroon as bribes. Fresenius garnered $56.7 million in proceeds from its improper payments in West Africa.

b. Resolution

Fresenius voluntarily disclosed the misconduct to the DOJ. Under the DOJ's Corporate Enforcement Policy, Fresenius was therefore eligible for a declination or a reduction of up to 50% off the bottom of the U.S. Sentencing Guidelines fine range. Fresenius's $84.7 million monetary penalty represents a reduction of 40% off the bottom of the U.S. Sentencing Guidelines fine range. The NPA is not explicit as to why Fresenius did not receive the full benefits of voluntary disclosure under the Corporate Enforcement Policy. However, two clues were offered. First, the DOJ noted the nature and seriousness of the offense, including that the misconduct was pervasive throughout a business unit of Fresenius, continued until 2016, and involved high-level executives. Second, the DOJ suggested that Fresenius deserved only partial credit for its cooperation. Although Fresenius conducted a thorough internal investigation, provided regular factual presentations to the DOJ, made foreign employees available for interview, and took other appropriate steps, the DOJ found that Fresenius did not timely respond to certain requests and did not always provide fulsome responses to requests for information.

6. Insurance Corporation of Barbados: Inniss, Innes, and Tasker

Key Facts:

Agencies: DOJ
Countries Involved: Barbados
Means of Corruption: Third party payments
Notes: The DOJ declined to prosecute ICBL, in part because it managed to charge all of the individuals involved in the conduct

On August 6, 2018, U.S. federal prosecutors unsealed an indictment charging former Barbados politician, Donville Inniss, with conspiracy and money laundering in connection with a bribery scheme in Barbados. Prosecutors subsequently added Ingrid Innes and Alex Tasker, former executives of Insurance Corporation Barbados Limited ("ICBL"), to the indictment.

ICBL is an insurance company headquartered in Barbados that offers various financial products, including life, property, and casualty insurance. Inniss, a United States lawful permanent resident, was a member of the Parliament of Barbados and the Minister of Industry, International Business, Commerce, and Small Business Development. Innes, a citizen of Canada, was the Chief Executive Officer of ICBL. Tasker, a citizen of Barbados, was a senior vice president of ICBL.

The second superseding indictment alleges that Innes and Tasker laundered approximately $36,000 in bribes through the United States to Inniss in exchange for his assistance in securing government contracts for ICBL. These bribes were funneled through the New York Dental Company, a company incorporated in New York with an address in Elmont, New York.

a. Overview of Conduct

The second superseding indictment alleges that between 2015 and 2016, Inniss leveraged his position as Barbados' Minister of Industry and engaged in a scheme to accept a total of $36,000 in bribes from ICBL, in violation of Barbadian law, and launder that money to and through the United States. In 2015, Inniss used his position as Minister of Industry to cause the Barbados Investment and Development Corporation ("BIDC") to renew an insurance contract with ICBL. The contract required BIDC to pay a premium of approximately

$330,734.65 to ICBL. Inness and Tasker agreed to pay Inniss five percent of the contract premium, or approximately $16,000, to ensure the BIDC renewed its contract with ICBL. To conceal the bribe payment, Innes and Tasker caused ICBL's majority shareholder to transfer $16,000 to a United States bank account in the name of New York Dental Company, which had no actual business with ICBL. ICBL's parent company was unaware of the scheme and believed the payment was made for consulting services based on a false invoice provided by Innes, Tasker, and another ICBL executive. The New York Dental Company then transferred $16,000 to a bank account in the United States in the name of Inniss.

Around March 2016, Inniss allegedly used his position to cause BIDC to renew another insurance contract with ICBL. ICBL employees including Innes and Tasker agreed to pay Inniss $20,000 and again caused ICBL's parent company to transfer the funds to the New York Dental Company bank account based on a false invoice provided by Innis, Tasker, and an ICBL executive. In April 2016, the New York Dental Company made transfers of approximately $9,000, $8,000, and $2,750 to Inniss' bank account in the United States.

b. Charges

The second superseding indictment charges Innis, Innes, and Tasker with one count of conspiracy to launder money with intent to carry on an offense against a foreign nation involving bribery of a public official, in violation of the Barbados Prevention of Corruption Act, and two counts of money laundering. The indictment also requires forfeiture of any property involved in the offenses. Trial for defendant Inniss is scheduled to begin on October 28, 2019.

On August 23, 2018, the DOJ announced that it had declined to prosecute ICBL under the FCPA Corporate Enforcement Policy. The DOJ reached this conclusion based on a number of factors: (1) ICBL's timely and voluntary self-disclosure; (2) ICBL's thorough internal investigation; (3) ICBL's cooperation with the DOJ; (4) ICBL's agreement to disgorge all profits made from the illegal conduct, amounting to $93,940.19; (5) steps ICBL has taken to enhance its internal compliance program; (6) ICBL's remediation measures, including termination of all employees involved in the misconduct; and (7) the fact that the DOJ has been able to identify and charge the culpable individuals.

7. Juniper Networks

Key Facts:

Agencies: SEC
Countries Involved: Russia, China
Amount of Total Financial Settlement: $11.7 million
Means of Corruption: Excessive discounts to resellers; travel and entertainment

On August 29, 2019, Juniper Networks, Inc. ("Juniper") agreed to a negotiated cease and desist order with the SEC to resolve charges that Juniper violated the internal accounting controls and record keeping provisions of the FCPA in connection with conduct in Russia and China. Juniper neither admitted nor denied the SEC's allegations, but agreed to pay a total of approximately $11.7 million in disgorgement, civil penalty, and prejudgment interest. The DOJ, which also investigated Juniper in connection with this conduct, closed its investigation in late 2017 without bringing charges.

Juniper is a California-based technology company that designs, manufactures and sells networking equipment products and services. According to the SEC, from 2008 to 2013 employees of Juniper's wholly-owned subsidiary who were based in Russia gave excess discounts to their resellers in order to create slush funds that could be used to provide improper benefits to clients, including some who were public officials. Although the employees informed Juniper's management that

the extra discounts were necessary to meet competition, in reality the employees and resellers allegedly wished to use the excess discounts to create pools of off-the-books funds that would be maintained by the resellers. These funds were then allegedly used, at least in part, to fund leisure trips for the employees of end-user clients in order to win or maintain business. The trips included, for example, travel to destinations such as Italy, Portugal, and various U.S. cities were there were no Juniper facilities. According to the SEC, communications reflect employees discussing their desire to provide these trips to ensure that would win business with the end-users.

The SEC indicated that in late 2009, a member of senior management learned that the employees in Russia were creating off-book accounts funded in part by the increased discounts. Although Juniper instructed the employees to discontinue these practices, it allegedly did not take effective measures to prevent this conduct, and the scheme continued through 2013.

The SEC also alleged that between 2009 and 2013, certain employees of Juniper's subsidiary in China provided domestic travel and entertainment for end-user clients that was excessive and inconsistent with Juniper's internal policies. These employees allegedly falsified the agendas for these trips by understating the amount of entertainment involved in order to ensure that Juniper's Legal Department, and in some cases, the end-user's companies, would approve the trips. The SEC indicated that Juniper's legal staff also on occasion approved these events after they had already been conducted, in violation of Juniper's policies.

The SEC indicated that it agreed to resolve these charges through a negotiated cease and desist order given Juniper's cooperation and remedial efforts. Juniper disclosed facts developed during an internal investigation and voluntarily produced and translated documents to SEC staff. Juniper also revised its compliance policies and procedures, made improvements to its compliance function, created an independent and expert investigations function, and made other changes to improve its internal controls, including a compliance preview and pre-approval of non-standard discounts.

The cease and desist order required Juniper to pay $4 million in disgorgement, $1.25 million in prejudgment interest, and a civil penalty of $6.5 million.

8. Micronesia (Lyon and Halbert)

Key Facts:

Agencies: DOJ
Countries Involved: Micronesia
Means of Corruption: Vehicles; tuition for relatives; cash; travel
Notes: Lyon's plea is unique in that it involved charges of corrupt payments to foreign officials and government officials in Hawaii

In May 2019, Frank James Lyon, owner of a privately-held engineering firm in Hawaii (Lyon Associates Inc. ("Lyon Associates")), was sentenced to 30 months in prison after pleading guilty to a one-count criminal information charging him with conspiracy to violate the anti-bribery provisions of the FCPA and the anti-bribery provision concerning programs that receive federal funds (18 U.S.C. § 666). In July 2019, Master Halbert, a Micronesian government official, was sentenced to 18 months in prison and three years of supervised release for his role in the bribery scheme after pleading guilty to one count of conspiracy to commit money-laundering.

The charges against Lyon relate to efforts to win government contracts in Hawaii and the Federated States of Micronesia ("FSM"), including an airport improvement project in FSM funded in part by the United States Federal Aviation Administration ("FAA AIP Project"). Halbert was a government official in the FSM Department of Transportation, Communications and Infrastructure, who administered FSM's aviation programs and managed its airports. According to the plea agreement, between 2006 and 2016, Lyon and his co-conspirators paid approximately

$200,000 to FSM officials, including Halbert, in order to obtain approximately $7.8 million in contracts in FSM for Lyon Associates.

Lyon took several steps and utilized several methods to corruptly influence Halbert and other officials with influence over projects in FSM. For example, Lyon purchased a vehicle in Hawaii and shipped it to FSM for Halbert's use. Lyon paid for a trip for Halbert and his wife to Las Vegas, including cash *per diems* for the trip. Lyon made tuition payments for one of Halbert's relatives who was attending the University of Hawaii. Lyon also provided bribes in the form of cash payments and wire transfers of various amounts for the benefit of Halbert and other FSM officials with decision-making authority related to the FAA AIP Project.

The criminal complaint against Halbert details additional requests for corrupt payments, some of which appear to have been denied by Lyon or other executives at Lyon Associates. For example, the complaint alleges that in November 2015, Halbert emailed an executive of Lyon Associates asking for Lyon Associates to book and pay for a hotel room for Halbert and his family in Guam. The executive denied the request, indicating that only project reimbursable travel expenses were being approved at that time. Halbert continued to contact Lyon and his colleagues at Lyon Associates in the following months requesting various sums of money. Overall, according to court documents, in addition to the trip, car, and tuition, Lyon and his co-conspirators paid Halbert thousands of dollars in cash bribes in Hawaii, FSM, and elsewhere in connection with contracts on the FAA AIP Project.

Lyon and his co-conspirators also paid bribes totaling approximately $240,000 to employees of a Hawaiian governmental agency in order to obtain a $2.5 million contract for Lyon Associates. Lyon facilitated payments to these officials through a co-conspirator (referred to in Lyon's plea agreement as "Co-Conspirator 3") in cash and wire transfers. Co-Conspirator 3 was identified as an official of the Hawaiian state agency. Lyon engaged Co-Conspirator 3's relative as a consultant ostensibly to provide marketing services to Lyon Associates. Instead, Lyon and his co-conspirators used this individual as a conduit to bribe Co-Conspirator 3 and his colleagues at the Hawaiian state agency to obtain a $2.5 million contract in Hawaii. These bribes did not involve foreign government officials and this did not implicate the FCPA. However, because the Hawaii project received federal funds, Lyon was charged under 18 U.S.C. § 666, which among other things, makes it a federal crime to bribe state officials in connection with a program receiving more than $10,000 in federal funds.

9. Microsoft

Key Facts:

Agencies: DOJ; SEC
Countries Involved: Hungary, Saudi Arabia, Thailand, Turkey
Amount of Total Financial Settlement: $25.3 million
Means of Corruption: Excessive discounts to resellers; vendors connected to government officials; gifts and hospitality

On July 22, 2019, Microsoft Corporation ("Microsoft") and its Hungarian subsidiary paid a total of $25.3 million to resolve FCPA charges and allegations related to conduct in Hungary, Saudi Arabia, Thailand, and Turkey. Microsoft's Hungarian subsidiary, Microsoft Magyarország Számítástechnikai Szolgáltató és Kereskedelmi Kft. (MS Hungary), entered into a three-year non-prosecution agreement with the DOJ pursuant to which MS Hungary admitted, accepted, and acknowledged responsibility for its employees' conduct and agreed to pay $8.75 million in criminal penalties. Microsoft also consented to the SEC's entry of an administrative cease and desist order alleging violations of the FCPA's books and records and internal controls provisions related to the conduct of Microsoft subsidiaries in Hungary, Saudi Arabia, Thailand, and Turkey. Microsoft, without admitting or denying the SEC's findings, agreed to disgorge $13.78 million in profits and to pay $2.78 million in prejudgment interest to resolve the charges.

a. Hungary

According to the DOJ and SEC, between 2013 and 2015, senior executives and other employees of MS Hungary participated in a margin-inflation scheme in order to bribe Hungarian officials in connection with the sale of Microsoft software licenses to Hungarian government agencies. MS Hungary sold software at a discount to intermediary partners, who then sold the same software at a higher price to government officials. The “discounts” (some of which ranged between 30-40%) were in fact used to fund kickbacks paid to government officials. MS Hungary employees falsely told Microsoft that the discounts were necessary to complete the transactions. According to both the DOJ and the SEC, the scheme generated approximately $14 million in business.

The SEC also pointed to various service agreements MS Hungary entered into with third parties for which MS Hungary conducted no due diligence and for which there existed very little evidence of actual services performed. In one particular case, MS Hungary engaged a vendor at the specific request of officials at Hungary’s National Tax and Customs Administration (MS Hungary’s end customer). In response to concerns raised about the competence of the vendor, an MS Hungary employee involved in the transaction stated that it was impossible to replace the vendor because”[it] is not simply a partner, it is THE PARTNER” (emphasis in original).

b. Saudi Arabia, Thailand, and Turkey

The SEC alleged that a similar scheme to the one perpetrated by MS Hungary was conducted by Microsoft’s subsidiary in Turkey. Specifically, according to the SEC, on at least one public tender for Turkey’s Ministry of Culture in July 2014, Microsoft’s Turkish subsidiary granted a larger than usual discount and engaged a third party intermediary whose services were not clearly recorded.

The improper conduct, as alleged by the SEC, of other Microsoft subsidiaries related mainly to the provision of gifts and hospitalities. Specifically, the SEC alleged that between 2012 and 2014, Microsoft’s Saudi Arabian subsidiary provided government officials with lavish gifts and travel opportunities by diverting at least $440,000 originally intended to be used for marketing and developing business proposals with Microsoft’s partners. Similarly, according to the SEC, between 2013 and 2015, Microsoft’s Thailand subsidiary provided more than $100,000 in gifts and travel to employees of non-government banking customers. Similar to the Saudi Arabian scheme, these gifts and travel opportunities were funded by money diverted from training programs into a slush fund.

c. Resolution

Hungary received a 25% reduction off the bottom of the applicable U.S. Sentencing Guidelines fine range for cooperating with the DOJ’s investigation and for “taking extreme remedial measures,” including terminating four licensing partners and implementing an enhanced and company-wide system of anti-corruption compliance. Microsoft’s enhanced internal controls included the development and use of data analytics to help identify high-risk transactions.

The SEC also acknowledged Microsoft’s cooperation with its investigation and Microsoft’s remedial measures and enhanced internal controls.

10. Mobile TeleSystems PJSC

Key Facts:

Agencies: DOJ; SEC
Countries Involved: Uzbekistan
Amount of Total Financial Settlement: $850 million
Means of Corruption: Business transactions with shell companies
Notes: Including amounts paid by MTS, Telia, and Vimpelcom, Karimova allegedly received more than $800 million in bribes

On March 7, 2019, the Department of Justice ("DOJ") announced that Mobile TeleSystems PJSC ("MTS") and its wholly owned Uzbek subsidiary, Kolorit Dizayn Ink LLC ("Kolorit") agreed to pay a combined $850 million in order to resolve the DOJ's investigation into an Uzbek telecommunications bribery scheme. MTS entered into a three-year deferred prosecution agreement ("DPA") related to one count of conspiracy to violate the anti-bribery and books and records provisions of the FCPA and one count of violating the internal controls provisions of the FCPA. Kolorit pled guilty to a one-count criminal information charging Kolorit with conspiracy to violate the anti-bribery and books and records provisions of the FCPA. A day earlier, on March 6, 2019, MTS consented to the SEC's cease and desist order related to the same conduct and agreed to pay a $100 million civil monetary penalty (credited toward the $850 million penalty imposed by the DOJ). In connection with the cease and desist order, MTS neither admitted nor denied the SEC's allegations that MTS violated the anti-bribery, books and records, and internal control provisions.

The DOJ also announced charges against former Uzbek official Gulnara Karimova and Bekhzod Akhmedov, a former executive of an Uzbek telecommunications company purchased by MTS (Uzdunrobita). The DOJ accused both of participating in a bribery and money laundering scheme that involved more than $865 million. Karimova, with Akhmedov's assistance, solicited bribes from MTS as well as other telecommunications companies, VimpelCom Limited ("VimpelCom"), and Telia Company AB ("Telia"), in exchange for her assistance in entering and operating in Uzbekistan's telecommunications market.

MTS is the largest mobile telecommunications company in Russia and an issuer of publicly traded securities in the United States. According to Assistant Attorney General Brian A. Benczkowski, the resolutions and indictments "demonstrate the Department's comprehensive approach to foreign corruption." He further stated that the Department "will aggressively pursue both corrupt foreign officials and the companies and individuals who bribe them in order to gain unfair business advantages, and . . . will do everything . . . to keep the proceeds of that corruption out of the U.S. financial system."

The DOJ's announcement marked the conclusion of a multinational effort to investigate and prosecute participants in the Uzbek bribery scheme, involving law enforcement authorities from the United States, Austria, Belgium, Cyprus, France, Ireland, Isle of Man, Latvia, Luxembourg, Norway, the Netherlands, Switzerland, Sweden, and the United Kingdom. At the time of the DOJ's announcement, neither Karimova nor Akhmedov was actually in the United States. Uzbek authorities imprisoned Karimova a day before the DOJ charged her, while Akhmedov had already fled to Russia. The DPA with MTS is the third resolution arising out of this bribery scheme. VimpelCom and its Uzbek subsidiary, Unitel LLC, entered into a resolution with the DOJ in 2016, and Telia and its Uzbek subsidiary, Coscom, in 2017.

a. MTS Bribery Scheme

Between 2004 and 2012, Karimova and Akhmedov engaged in an extensive bribery scheme in which Akhmedov solicited and facilitated corrupt bribe payments from telecommunications companies seeking to enter the Uzbek market. In exchange, Karimova allegedly used her influence over Uzbek authorities, both as an Uzbek official and as the daughter of Uzbekistan's then-President Islam Karimov, to help these companies obtain and retain

lucrative business opportunities in the Uzbek telecommunications market. Three companies, MTS, VimpelCom, and Telia, were involved, along with their Uzbek subsidiaries.

Between 2004 and 2012, Akhmedov conspired with others to pay more than $420 million to Karimova in exchange for her taking corrupt action to ensure MTS could enter, and continue to operate in, the Uzbek telecommunications market. These bribes were made through business transactions, often with Karimov's shell companies, that were made to look legitimate.

In the first stage of the scheme, MTS sought to enter the Uzbek market by acquiring Uzdunrobita, for which Akhmedov was the general director. MTS acquired a 33% stake in Uzdunrobita from a Karimova shell company and a 41% stake from an unnamed American company. MTS paid Karimova's shell company six times per share (totaling $100 million) what it paid to the American company, even though the shares were identical. MTS and Karimova's shell company also entered into an option agreement that gave MTS the option to buy, and the shell company the option to sell, the shell company's remaining 26% stake in Uzdunrobita for $37.7 million, plus interest, over three years. MTS's board retroactively approved these agreements in violation of its own policies.

In 2006, Karimova and Akhmedov negotiated an amendment to the option agreement between MTS and Karimov's shell company to eliminate MTS's option to buy, extend the shell company's option to sell, and replace the fixed price with a yet-determined market value as calculated by an international investment bank. Because Uzdunrobita's value had substantially increased in part due to Karimova's influence, Akhmedov and MTS management understood that this agreement conferred significant benefits on Karimova. In 2007, Karimova caused her company to notify MTS it intended to exercise its option, securing the bribe payment to Karimova. An investment bank determined the shell company's 26% interest was worth $250 million, and in June that year, MTS's board of directors approved a $250 million payment to the shell company's bank account in Hong Kong.

In the second stage of the scheme, Karimova sought additional bribes from MTS and Uzdunrobita, demanding that Uzdunrobita extend $113 million in purported loans to help her buy a stake in a bank. When MTS did not agree to the loans, Karimova threatened to interfere with Uzdunrobita's operations. In the summer and fall of 2008, Akhmedov and MTS management arranged to pay $30 million in bribes to Karimova, using an MTS subsidiary to enter into a sham contract with the subsidiary of another one of Karimova's shell companies. The contract provided that the MTS subsidiary would pay $30 million in exchange for Karimova's shell company repudiating its ownership of certain telecommunications frequencies, which were then reassigned to Uzdunrobita by the Uzbek government. In August 2008, the MTS subsidiary and Karimova's shell company executed the contract, and within days the Uzbek government issued an order reallocating frequencies held by the subsidiary to Uzdunrobita. MTS or its subsidiary then paid $30 million to the shell company's bank accounts.

In the third stage of the scheme, between late 2008 and early 2009, Akhmedov and MTS management discussed acquiring Kolorit, an Uzbek advertising company, as a mechanism to funnel additional bribes to Karimova. Karimova owned and controlled Kolorit, though Kolorit was nominally owned by another entity. However, MTS's Department of Strategic Planning rejected Kolorit's acquisition because it was not part of MTS's core business and the estimate for Uzbek advertising market development was not realistic. Multiple internal and external valuations found Kolorit was worth significantly less than the recommended purchase price. Nevertheless, in 2009, Akhmedov and MTS management approved MTS's acquisition of Kolorit, paying Kolorit's nominal shareholders approximately $40 million.

In the fourth and final stage of the scheme, Karimova solicited additional bribes from MTS and Uzdunrobita through Akhmedov, including $1.1 million to purported charities and sponsorships that were really for Karimova's benefit. These payments occurred in violation of MTS's internal control procedures that required preapproval of such payments.

By the end 2012, the Uzbek government expropriated Uzdunrobita as a result of its failure to meet Karimova's demands for additional payments.

b. Resolution

The $850 million financial penalty imposed on MTS and Kolorit is approximately 25% above the low-end of the Sentencing Guidelines. Of that amount, $40 million will constitute a forfeiture and $500,000 a criminal fine paid by MTS on behalf of Kolorit. The DPA further specifies that the $850 million payment will be offset by up to $100 million for any civil fines paid by MTS to the SEC. The DOJ listed several factors that it considered in determining an appropriate penalty for MTS: (1) MTS did not voluntarily and timely self-disclose; (2) MTS's level of cooperation was lacking –it significantly delayed production of documents, refused to support interviews, and failed to take disciplinary measures with respect to executives and employees involved in the misconduct; (3) the nature and seriousness of the crimes. In terms of mitigating factors, the DOJ considered that the Uzbek government had expropriated MTS's assets in Uzbekistan such that the company had no pecuniary gain.

The DOJ noted that MTS had taken steps to enhance its compliance program and internal accounting controls but because the program had yet to be fully implemented and tested, an independent compliance monitor would be required to reduce the risk of future misconduct. As part of its DPA, MTS agreed to retain a monitor for a period of three years.

Karimova and Akhmedov face charges of conspiracy to commit money laundering, while Akhmedov also faces one charge of conspiracy to violate the FCPA and two charges of violating the FCPA. The indictment also includes forfeiture allegations that require Karimova and Akhmedov to forfeit property traceable to their money laundering conspiracy and Akhmedov was also required to forfeit property traceable to the commission of his FCPA offenses.

11. Mozambique Fraud/Privinvest

Key Facts:

Agencies: DOJ
Countries Involved: Mozambique
Notes: Similar to the 1MDB scheme, defendants financed large amounts from large banks (backed by the state) and then simply took hundreds of millions of dollars from the amounts raised/borrowed

On March 7, 2019, the DOJ unsealed a four-count indictment charging two executives of a shipbuilding company, three former senior Mozambican government officials, and three former London-based investment bankers for their roles in a $2 billion fraud, money laundering, and corruption scheme involving loans guaranteed by the government of Mozambique.

The defendants in this ongoing enforcement action are: (i) Manuel Chang, the former Minister of Finance for Mozambique; (ii) Antonio do Rosario, a former official with the Mozambique State Information and Security Service and director of three Mozambican entities used in the scheme; (iii) Teofilo Nhangumele, a former official at the Office of the President of Mozambique; (iv) Jean Boustani, a former lead salesman for Privinvest Group, a United Arab Emirates-based shipbuilding company; (v) Najib Allam, the former CFO of Privinvest; (vi) Andrew Pearse, a former Managing Director of Credit Suisse; (vii) Surjan Singh, a former Managing Director of Credit Suisse; and (viii) Detelina Subeva, a former Vice President of Credit Suisse.

All eight defendants were charged with conspiracy to commit wire fraud and conspiracy to commit money laundering. All defendants except Nhangumele were also charged with conspiracy to commit securities fraud, and

Pearse, Surjan, and Subeva (the three bankers) were charged with conspiracy to violate the anti-bribery and internal controls provisions of the FCPA.

According to the DOJ, from 2013 to 2016, three Mozambican state-owned entities, ostensibly created to undertake maritime projects in Mozambique, took out loans of more than $2 billion that were guaranteed by the Mozambican government. The entities were ProIndicus, Empresa Moçambicana de Atum (EMATUM), and Mozambique Asset Management (MAM). All three companies were created right before the loan transactions and shared the same CEO, Antonio do Rosario, who was a senior official in Mozambique's security services. The loans were purportedly to be used to fund maritime projects for which Privinvest, a UAE-based shipbuilder, would provide equipment and services. The companies were meant to undertake work that included coastal surveillance, tuna fishing, and building and maintaining shipyards. According to press reports, the loans were arranged by the London offices of Credit Suisse, and by VTB bank, a Russian investment bank owned by the Russian government. EMATUM borrowed $850 million, ProIndicus $622 million, and MAM $535 million, totaling just over $2 billion. Chang, acting as Minister of Finance, signed guarantees on behalf of Mozambique for all three loans. Virtually all proceeds from the loans were paid directly to Privinvest.

The charging documents indicate that Privinvest diverted more than $200 million in loan proceeds for illicit purposes, including bribe payments to Chang and other Mozambican officials, and kickback payments to Privinvest personnel and the bankers. The banks themselves also allegedly received hundreds of millions of dollars in fees for arranging the loans. The companies allegedly funneled the improper payments through Privinvest by paying inflated prices for equipment and services, and Privinvest then distributed bribes and kickbacks to the bankers and the public officials involved in the scheme. The DOJ indicated that the defendants also defrauded investors and potential investors in the financings through numerous material misrepresentations and omissions, including regarding the use of the loan proceeds, the amount and maturity dates of debt owed by Mozambique, and Mozambique's ability to repay the investors.

The conspirators, and particularly Chang, are also accused of seeking to hide the existence of these loans from Mozambique's international creditors. At the end of 2012, Mozambique had approximately $6 billion in national debt, and the International Monetary Fund ("IMF"), a major donor to Mozambique, was concerned that this was an unsustainably high debt level. Allegedly to circumvent the IMF's restrictions on new public debt, then-Minister of Finance Chang kept the new loans off of Mozambique's balance sheet.

Once the loans were discovered, the IMF and other international donors halted their payments to Mozambique, sending the Mozambican economy into disarray. Mozambique ultimately defaulted on its loan obligations in January 2017, and has been working with international creditors to restructure its debt ever since. The IMF estimates that Mozambique will not be able to make payments on its external debt until 2023, when natural gas production from the Rovuma Basin is set to begin.

Subeva, Pearse, and Singh were all arrested in the U.K. in January 2019. Authorities in the U.S. initially planned to extradite the three to the U.S. to stand trial, but they each ultimately negotiated plea agreements. In May 2019, Subeva pled guilty to the money laundering conspiracy charge. She was followed shortly thereafter by Pearse in July 2019, and Singh in September 2019, both of whom similarly pled guilty to one count of conspiracy to commit money laundering.

As of October 2019, Jean Boustani was being held in the U.S. as he awaits trial. Manuel Chang, the former Minister of Finance, is detained in South Africa as South African courts consider separate extradition requests from Mozambique and the United States. South African authorities initially planned to extradite Chang to Mozambique. However, press reports indicate that South Africa's new Justice Minister is skeptical of Mozambique's extradition request Chang's potential immunity and the lack of charges to date. Antonio do Rosario

and Teofilo Nhangumele were reportedly arrested by the Mozambican authorities and are awaiting trial in Mozambique. Najib Allam remains at large.

12. TechnipFMC

Key Facts:

Agencies: DOJ; SEC
Countries Involved: Brazil; Iraq
Amount of Total Financial Settlement: More than $300 million
Means of Corruption: Third-party agent
Notes: Related to DOJ's 2017 resolution with Keppel Offshore

On June 25, 2019, TechnipFMC plc ("TechnipFMC"), a U.K.-based oil and gas services company whose shares are traded publically on the NYSE, entered into a three year DPA with the DOJ to resolve allegations that TechnipFMC's predecessor entities, Technip S.A. ("Technip") and FMC Technologies, Inc. ("FMC"), each engaged in separate conspiracies to violate the anti-bribery provisions of the FCPA. According to the DOJ, Technip engaged in corrupt conduct in Brazil and FMC engaged in corrupt conduct in Iraq. TechnipFMC's wholly-owned U.S. subsidiary, Technip USA, Inc. ("Technip USA"), also pled guilty to one count of conspiracy to violate the anti-bribery provisions of the FCPA in connection with the conduct in Brazil.

As part of its settlement with the DOJ, TechnipFMC agreed to pay a total criminal fine of more than $296 million. Approximately $214 million of this amount will be paid to Brazilian authorities as part of TechnipFMC's settlement with the Advogado-Geral da União, the Contraoladoria-Geral da União and the Ministério Público Federal, with the remaining approximately $82 million applied to the U.S. settlement.

Four months later, on September 23, 2019, TechnipFMC consented to the entry of an SEC cease and desist order related to violations of the anti-bribery, books and records and internal controls provisions of the FCPA in connection with FMC's conduct in Iraq. In its settlement with the SEC, TechnipFMC agreed to pay an additional approximately $4.3 million in disgorgement, and just under $735,000 in prejudgment interest.

a. Conduct in Brazil

Between 2003 and 2014, Technip and Technip USA engaged in a conspiracy to bribe officials from Petrobras and the then-ruling Worker's Party of Brazil in order to secure a number of offshore oil and gas projects. The majority of the misconduct in Brazil involved a joint venture between Technip USA and a subsidiary of Keppel Offshore & Marine Ltd. ("Keppel"), a Singapore-based contractor that specializes in shipbuilding and offshore rig design and construction. Keppel previously settled allegations related to this same conduct with authorities in the United States, Brazil and Singapore.

According to the DPA, beginning around 2003, the joint venture entered into a number of agreements with companies tied to a consultant in Brazil that had a prior relationship with Keppel. In total, Technip and Keppel paid more than $69 million in commissions to the agent under these agreements. The agent kept a portion of these payments for himself and transferred the rest to two Petrobras employees and to officials from the Workers' Party in order to ensure that the joint venture was awarded a number of oil and gas platform projects. Some of these payments were initially made by a Technip subsidiary through its bank account in New York. Beginning around 2009, in order to avoid Technip's internal due diligence processes, Technip and Keppel altered the structure of the payments to the agent so that they would be made solely by a Keppel subsidiary. Keppel then invoiced the joint venture for Technip's portion of the corrupt payments. The joint venture also made direct payments to the Workers' Party and certain Workers' Party political candidates.

In total, Technip and its subsidiaries earned more than $135 million in profits from the corruptly obtained business in Brazil.

b. Conduct in Iraq

In Iraq, FMC engaged in a scheme together with a Monaco-based oil and gas services intermediary to make improper payments to officials from the state-owned South Oil Company of Iraq and Missan Oil Company of Iraq to help secure seven contracts involving the provision of metering technologies.

According to the DPA, between 2008 and 2013 FMC entered into multiple agency agreements with the Monaco-based intermediary in order to facilitate the bribery scheme. This intermediary made improper payments either directly to Iraqi officials or to other third parties who passed the payments on to Iraqi officials. FMC then reimbursed the intermediary for these payments through the phony agency agreements. The agency agreements often called for conspicuously large commission payments, typically between eight to ten percent of the contract value, and in one instance reaching up to 12 percent of the contract value.

In total, FMC Technologies earned approximately $5.3 million from the corruptly obtained business in Iraq.

c. Resolution

According to the DOJ, TechnipFMC's criminal fine was reduced by 25% from the bottom of the applicable U.S. Sentencing Guidelines range based in large part on the TechnipFMC's substantial cooperation with the DOJ and extensive remediation efforts. The SEC cited similar factors in its decision to resolve the allegations against TechnipFMC through a negotiated cease and desist order. Among other things, TechnipFMC was commended for conducting a thorough internal investigation, cooperating with the DOJ and SEC's investigations, making regular factual presentations to the DOJ, and producing documents to the DOJ from foreign countries in ways that did not implicate foreign data privacy laws. TechnipFMC also engaged in remedial measures that included implementing heightened controls and additional procedures relating to third parties, conducting ongoing reviews of its compliance program, and providing additional training to employees and third parties.

Under the terms of the DPA, TechnipFMC agreed to submit three annual reports to the DOJ regarding its ongoing efforts to improve its compliance program and internal controls. TechnipFMC similarly committed to submitting three reports to the SEC describing these efforts and improvements.

13. Telefônica Brasil S.A.

Key Facts:

Agencies: SEC
Countries Involved: Brazil
Amount of Total Financial Settlement: $4.125 million
Means of Corruption: Hospitality (World Cup and Confederations Cup tickets)

On May 9, 2019, Telefônica Brasil S.A. ("Telefônica Brasil"), a subsidiary of Spanish multinational broadband and telecommunications provider Telefónica S.A., consented to an administrative cease and desist order and agreed to pay $4.125 million as part of a settlement with the SEC relating to Telefônica Brasil's violations of the FCPA's internal accounting controls and recordkeeping provisions.

The alleged misconduct related to a hospitality program, as part of which Telefônica Brasil offered tickets to high-end soccer events to (and thereby allegedly attempted to curry favor with) public officials overseeing decisions immediately impacting its business. According to the SEC, Telefônica Brasil mischaracterized these payments in their books and records and failed to maintain a system of internal controls.

a. Relevant Conduct

In March 2012, Telefônica Brasil allegedly purchased 1,860 tickets to the 2014 Men's World Cup in Brazil for a total of approximately $5.1 million, to be paid in three annual installments. The SEC alleged that Telefônica Brasil allocated approximately 10 percent of the tickets to the Institutional Relations Department ("IR Department"), which interacted with the Brazilian government and foreign governments. Telefônica Brasil, primarily through the IR Department, allegedly gave a total of 194 World Cup tickets to 93 government officials. The total value of tickets and related hospitality given to these government officials amounted to $621,576.

Telefônica Brasil allegedly gave tickets to government officials who had influence over policy decisions that directly affected its business interests, including federal congressmen, senators, mayors, and other officials. Emails throughout June and July 2014 suggest that management considered past support from the officials and the potential need for future support on issues pertinent to the company. For example, the emails show that tickets were requested for a federal legislator's chief of staff because there was legislative activity "going through the House" and Telefônica Brasil staff expressed that they "will need his help." A free trade tax zone official who received a ticket was asked for his "ongoing support" in receiving customs clearance. Similarly, an email between IR Department employees suggested inviting two Brazilian mayors only if they had the opportunity to speak with them about certain "legislative amendments" which directly affected Telefônica Brasil.

In March and April 2013, Telefônica Brasil also allegedly purchased 240 tickets for the Confederations Cup in Brazil (worth $428,219). According to the SEC, approximately 15% of these tickets were given (via the IR department) to government officials, including federal congressmen and various government ministry officials, who had direct influence over policy decisions that directly affected Telefônica Brasil's business interests. The total value of tickets and related hospitality given to government officials allegedly amounted to $117,230.

The SEC determined that Telefônica Brasil lacked sufficient controls to prevent employees from participating in bribery schemes, and employees circumvented the controls that were in place. Telefônica Brasil had a general code of ethics that prohibited offering or accepting incentives "which may reward or influence a business decision," and Telefônica Brasil prohibited donations linked with political activity. However, the internal accounting controls focused on employees accepting tickets and hospitality, as opposed to offering them to government officials. As a result, despite inquiries about the policy's applicability to this situation, Telefônica Brasil offered such tickets and hospitality to government officials with the approval of senior managers.

According to the SEC, Telefônica Brasil's recordkeeping did not properly characterize the purchase of tickets and related hospitality that were given to government officials. The paperwork seeking internal approval to purchase the World Cup tickets did not mention that tickets would be given to government officials, even though that purpose was generally known within the company. When Telefônica Brasil paid for its tickets for the two events in five total installments, those expenses were characterized as either "Publicity Institutional Events" or "Advertising & Publicity," without mention that the tickets and hospitality were used for government officials. According to the SEC, Telefônica Brasil's recordkeeping therefore did not "accurately and fairly reflect the transactions and dispositions of the company's assets."

b. Remedial Acts and Cooperation

The SEC credited Telefônica Brasil for its remedial action and cooperation in the SEC's investigation. Telefônica Brasil cooperated by sharing facts of its internal investigation and voluntarily producing and translating documents. Telefônica Brasil also pursued remedial action by adopting a new anticorruption policy, improving its compliance functions, and enhancing its internal accounting controls.

14. Quad/Graphics

Key Facts:

Agencies: SEC
Countries Involved: Peru; China
Amount of Total Financial Settlement: $9.895 million
Means of Corruption: Fake vendors, law firm, sales agents

On September 26, 2019, the SEC announced that Quad/Graphics Inc. ("Quad"), a publicly listed, Wisconsin-based digital and print marketing provider, agreed to pay nearly $10 million to resolve charges that it violated the FCPA's anti-bribery, books and records, and internal controls provisions by engaging in multiple bribery schemes in Peru and China. The SEC filed a cease and desist order against Quad, which neither admitted nor denied the SEC's findings. Quad agreed to pay $6,936,334 million in disgorgement, $959,160 in prejudgment interest, and $2 million in civil penalties for a total of $9,895,334. Quad's settlement with the SEC, which took into consideration Quad's voluntary disclosure, cooperation, and remedial efforts, was announced one week after the DOJ issued a formal letter declining to prosecute Quad for the same underlying conduct.

a. Summary of charged conduct

In 2010, Quad acquired World Color Press, Inc. ("World Color"), a Canadian printing company. Prior to that, Quad's business had been focused almost entirely on domestic sales. With the acquisition of World Color, Quad became an international business with significant foreign sales. According to the SEC, Quad's subsidiary in Peru ("Quad Peru"), which had previously been a World Press subsidiary, engaged in multiple bribery schemes. First, from 2011 to 2016, Quad Peru paid an individual with influence in the Peruvian government to increase sales with Quad's largest governmental customers, including INEI. The bribe payments (representing approximately 13% of each government contract), were made through sham vendor companies, all of which were owned by the said individual. Among other things, the SEC alleged that a U.S.-based Finance Executive for Latin America, despite having been notified of concerns by local staff, ignored significant red flags relating to the sham vendors' fake invoices, including rounded dollar amounts, large and disproportionate invoice amounts, consecutively numbered invoices (at times with same date), and invoices provided without proof of services or purchase orders. The U.S.-based Finance Executive only reported concerns to his supervisor and Quad's Legal Department in 2016, after a new local Senior Finance Manager declined to approve the problematic invoices.

According to the SEC, Quad Peru also engaged in a judicial bribery scheme, related to a $12 million VAT dispute with the Peruvian Tax Authority. Specifically, the SEC alleged that Quad Peru paid bribes through a local Peruvian law firm, engaged to represent Quad Peru in the tax dispute, to influence local judges in their decisions in the dispute.

According to the SEC, prior to its acquisition by Quad, World Press (a Canadian company) regularly conducted business with Cuba, including with ETECSA, a Cuban state-owned telecommunications company that purchased telephone directories from World Press' Peruvian subsidiary. The SEC alleged that for a period of more than two years after Quad acquired World Press, Quad Peru continued sales to ETECSA, despite the fact that such sales were prohibited for Quad under U.S. sanctions and export control laws. In order to conceal these transactions, the SEC alleged that Quad employees in Peru and the U.S. falsified records, including shipping documents, invoices, and journal entries. The SEC alleged that a U.S.-based Operations Executive worked with Quad Peru's General Manager and Senior Finance Manager to conceal the Cuban business, going as far as to purposely mislead Quad's Legal Department that Quad Peru was no longer working with Cuba. According to the SEC, the falsification of these records was a violation of the FCPA's books and records provision.

According to the SEC's order, Quad also engaged in bribery schemes to secure business through its Chinese subsidiary, Quad/Tech Shanghai Trading Company ("Quad China"). Specifically, Quad China allegedly paid or

promised to pay approximately $182,000 in improper commissions to sham sales agents, who then passed on some of these commissions to employees of private and government-owned customers in order to induce increased sales from such customers. The SEC alleged that these payments were recorded in Quad's books and records as "commissions" while they were in fact bribes. Moreover, the SEC alleged that Quad China failed to conduct any due diligence on the sales agents that were used and obtained no proof of services before paying the invoices, which, according to the SEC was a failure to maintain adequate internal controls.

b. DOJ Declination

The DOJ declined to prosecute Quad on based on a multitude of factors set out in the Corporate Enforcement Policy, including (but not limited to) Quad's (i) prompt and voluntary self-disclosure of the misconduct (ii) thorough and comprehensive investigation and (ii) full and proactive cooperation. The DOJ also noted the fact the Quad had agreed to disgorgement of ill-gotten gains to the SEC, thereby further highlighting the enforcement agencies' greater coordination and departure from a practice of "piled on" enforcements.

15. Walmart

Key Facts:

Agencies: DOJ; SEC
Countries Involved: Brazil, China, India, Mexico
Amount of Total Financial Settlement: $282 million
Means of Corruption: Use of intermediaries

On June 20, 2019, Walmart Inc. ("Walmart") agreed to pay the DOJ and SEC approximately $282 million in order to resolve a seven-year investigation into conduct that occurred in its subsidiaries in Brazil, China, India and Mexico between 2000 and 2011. Walmart entered into a three-year non-prosecution agreement ("NPA") with the DOJ and agreed to a two-year monitorship. Relatedly, Walmart's wholly owned Brazilian subsidiary, WMT Brasilia, S.a.r.l. ("Walmart Brazil"), pleaded guilty to one count of causing a violation of the FCPA's books and records provisions. Walmart also consented to a cease and desist order ("Order") filed by the SEC in relation to charges that it violated the FCPA's books and records, and internal accounting controls provisions. In addition to the total penalty, the company reportedly spent about $900 million on legal fees, pre-resolution investigations and extensive compliance enhancements over the past seven years.

Headquartered in Bentonville, Arkansas, and ranked the world's largest company by revenue Walmart is a multinational retailer with an approximate global headcount of 2.2 million employees operating stores in 27 countries. Walmart's shares are publicly traded on the New York Stock Exchange, qualifying the company as an "issuer" under the FCPA.

According to admissions by Walmart and findings by the DOJ and SEC, from at least 2000 to 2011, despite numerous red flags and allegations brought to their attention through internal audits as well as whistleblower reports, Walmart's senior personnel repeatedly failed to remediate and implement sufficient anti-corruption related internal accounting controls in Walmart's subsidiaries in Brazil, China, India and Mexico. Among other things, Walmart's internal control failures allowed those foreign subsidiaries to hire inadequately vetted third-party intermediaries who ultimately made improper payments to government officials to obtain permits and licenses for the construction and operation of Walmart stores.

According to Assistant Attorney General Benczkowski, "Walmart profited from rapid international expansion, but in doing so chose not to take necessary steps to avoid corruption." Indeed, Walmart executives were made aware of corruption risks in certain of Walmart's foreign subsidiaries as early as 1999/2000, and received multiple audit

reports identifying weaknesses in anti-corruption controls in the years that followed. Despite these warnings, Walmart did not adopt a Global Anti-Corruption Policy until 2008, and thereafter did not ensure its adequate implementation, particularly by foreign subsidiaries. By 2009, Walmart moved away from a centralized approach of its anti-corruption program by adopting a new “Freedom within a Framework” standard, which allowed foreign subsidiaries to design their own compliance programs as long as they complied with certain global standards, but these standards appear not to have been set out in detail. Another Global Anti-Corruption Policy issued (in draft format) in 2010 left it to the foreign subsidiaries to determine “the appropriate level of due diligence required” for its third parties. It was not until 2011 that Walmart recognized the shortcomings of such a decentralized system and hired external legal counsel and other compliance experts to test the compliance program in various foreign subsidiaries, including those described below.

a. Overview of Conduct

i. Conduct in Mexico

The conduct of Walmart’s Mexican subsidiary (“Walmart Mexico”) involved two different and consecutive schemes, relating to (i) improper payments made to obtain real estate permits and licenses through third party intermediaries referred to as “gestores” and (ii) improper donations made directly to government officials.

The first scheme was reported to Walmart’s headquarters in 2005 through a whistleblower, who had previously been engaged as attorney in Walmart Mexico’s Real Estate department (“Whistleblower”). Specifically, the Whistleblower reported that - with the knowledge of several Walmart Mexico executives and lawyers - from about 1999 to 2004, he had directed intermediaries called “gestores” to make improper payments to government officials for obtaining real estate licenses and permits. Although Walmart, upon receiving the Whistleblower’s reports, hired outside counsel in Mexico and the United States to conduct preliminary interviews and draft an investigative plan, it charged its internal audit team with conducting the internal investigation. When the audit team’s investigative report identified potential violations of laws and recommended additional investigative steps, Walmart ignored these recommendations and ultimately tasked a senior internal attorney, whom the Whistleblower had identified as having known about the scheme while it had taken place, to lead on the investigation. Unsurprisingly, the final investigation report of the reportedly complicit senior internal attorney stated that no evidence existed to substantiate the corruption allegations. Walmart took no further steps to investigate the case.

Moreover, from at least 2006 until 2011, Walmart’s Mexico subsidiary increased its practice of donating goods and services to municipalities and other local governmental entities. Some of the goods donated, such as cars and computers, were capable of being converted to personal use. According to the SEC Order, such in-kind donations were also made around the time the Walmart Mexico obtained permits and licenses. Both the DOJ and the SEC noted that, despite being aware of corruption risks associated with intermediaries and donations, Walmart Mexico failed to implement adequate anti-corruption controls to guarantee that third-party intermediaries did not make improper payments to government officials or that goods donated to local governmental entities were not being converted to personal use.

ii. Conduct in Brazil

The conduct involving Walmart Brazil equally points to a disconnect between Walmart’s U.S. headquarters and its foreign subsidiaries. Although Walmart’s U.S. executives had been warned about corruption risks in Brazil as early as 2000, it failed to undertake concrete actions to adequately address these risks for several years. As a result, during a period of rapid expansion, Walmart Brazil retained and renewed contracts with high-risk third party intermediaries without conducting prior due diligence and improper payments were made by these intermediaries.

Specifically, in 2008, Walmart Brazil engaged a Brazilian construction company to build eight Walmart stores in Brazil for a total of $52 million. Despite the high-risk area and high contract value at stake, Walmart Brazil did not conduct due diligence on said construction company until one year later. The construction company then failed a multi-step due diligence process due to findings of "cases of corruption," prompting the Compliance Department of Walmart Brazil to advise that no further contracts were to be signed with the company. However, as there was no mechanism in place to effectively block a company that had failed the due diligence process, Walmart Brazil continued to use and pay the construction company, which, in turn, proceeded to make improper payments to public officials in connection with two store constructions in 2009.

Also in 2009, Walmart Brazil wished to retain the services of a highly-connected intermediary to assist in and accelerate the construction permits and licenses process related to store construction. However, Walmart Brazil executives were aware of several red flags surrounding the intermediary. For example, the intermediary was a former government official and provided her services as an individual rather than through a company. As a result, rather than hiring the intermediary directly, Walmart Brazil directed the construction company to hire the intermediary. The intermediary obtained all government approvals in a condensed time-frame, earning her the nickname of "sorceress" or "genie" within Walmart Brazil. Walmart Brazil falsely recorded $527,000 it knew and intended to go to the intermediary as payments to the construction company.

iii. Conduct in China

In China, from as early as 2003, a Walmart group internal audit report and audits by Walmart's Chinese subsidiary ("Walmart China) identified deficiencies in the subsidiary's anti-corruption related internal accounting controls. Among other things, an October 2006 China Subsidiary Practices Review report identified FCPA awareness and training deficiencies. No action was taken by Walmart China or U.S. executives to provide such training. Similarly, from at least 2007 onwards, Walmart senior employees in the U.S. knew or had reason to know that certain third party contracts with Walmart China lacked anti-corruption provisions and documentation of required due diligence. Walmart China only took action to improve its anti-corruption related internal accounting controls in 2011.

iv. Conduct in India

In 2006, before Walmart began operations in India, Walmart learned of corruption risks in connection with obtaining licenses and permits and with its local joint-venture partner. Between 2008 and 2011, Walmart received several audit reports discussing control deficiencies related to, among others, the absence of a formal third party due diligence process, third-party contracts lacking FCPA provisions, disbursements that had no supporting documents and insufficient FCPA training for employees. In addition, Walmart's senior executives received a whistleblower report alleging improper payments made by the Indian joint venture to government officials to obtain store operating permits and licenses. Yet, Walmart and the Indian joint venture failed to address anti-corruption concerns and never investigated the whistleblower allegations. Because of Walmart's failure to implement sufficient anti-corruption internal accounting controls, from 2009 through 2011, Walmart's store operators in India were able to retain intermediaries who made improper payments to government officials to obtain store operating permits and licenses, which were recorded in the joint venture's books and records with vague descriptions (e.g., "miscellaneous," "incidental," and "government fee").

b. Resolution

Both the DOJ and SEC positively noted the "significant" remedial measures taken by Walmart, including enhancing its global anti-corruption compliance program and internal anti-corruption accounting controls, hiring

several compliance personnel, and implementing an automated global license management system and a global donation management system.

Walmart agreed to pay a criminal fine of $138 million as part of its NPA. Walmart Brazil, pleaded guilty to a single count of violating the FCPA's books and records provision. In addition, Walmart agreed to retain a compliance monitor for two years, whose mandate is restricted to evaluating the company's compliance program for key risk areas (e.g., licenses and permits) in four countries and Walmart's home office.

The DOJ granted Walmart a 25% discount off the bottom of the U.S. Sentencing Guidelines fine range for the portion of the penalty related to conduct in Brazil, China and India, and a 20% discount for the portion of the penalty related to the conduct in Mexico. The reduction was granted to Walmart on the basis of its cooperation with U.S. authorities and its significant remediation efforts. Walmart received only partial cooperation credit for conduct in Mexico, because, according to the DOJ, the company did not timely provide information to the government and failed to de-conflict with the government's request to interview one witness.

In connection with its resolution with the SEC, Walmart agreed to pay a total of $144.7 million, including $119,647,735 in disgorgement and $25,043,437 in prejudgment interest. The company also agreed that, over a two-year time period, it would report to the SEC on its remedial efforts and share with the SEC any external audit reports generated during said two-year period.

16. Westport Fuels Systems

Key Facts:

Agencies: SEC
Countries Involved: China
Amount of Total Financial Settlement: $4.1 million
Means of Corruption: Joint ventures

On September 27, 2019, the SEC filed a cease and desist order against Vancouver-based Westport Fuels Systems, Inc. ("Westport") and its former CEO, Nancy Gougarty for violations of the FCPA's anti-bribery, books and records, and internal controls provisions in connection with Westport's alleged bribery of a foreign official in China. Without admitting or denying the allegations, Westport agreed to disgorge $2.35 million and pay prejudgment interest of $196,000 plus a civil penalty of $1.5 million. Gougarty agreed to pay a civil penalty of $120,000.

Westport designs and manufactures fuel systems powered by natural gas, propane and hydrogen. According to the SEC, between 2013 and 2016, Westport engaged in a scheme to bribe a Chinese government official in order to obtain business and obtain a cash dividend from a Chinese joint venture between Westport and the state-owned entity where the official worked. The cease and desist order indicates that Westport transferred shares of stock in the Chinese joint venture at below market value to a private equity fund in which the official held a financial interest. In return, the official allegedly used his influence to authorize a cash dividend of 30% of undistributed profits from the joint venture, 20% more than what was provided for under the joint-venture agreement. The Chinese official also allegedly used his influence to cause the joint venture to enter into a long-term supply agreement with Westport that ultimately resulted in the joint venture purchasing approximately $500,000 of engine components from Westport.

Westport took steps to disguise the share transfer. When recording the share transfer in its books and records, Westport hid the involvement of the private equity fund. Westport falsely recorded the payment as received from an SOE related to the SOE where the official worked. Westport also reported in its SEC filings that the identity of the counterparty in the share transfer was this same SOE, rather than the private equity fund. Westport then failed to reconcile its public filings with the source documents that would have indicated that the true counterparty was the private equity fund.

The SEC indicated that it agreed to resolve these charges through a negotiated cease and desist order in light of Westport's cooperation with the SEC's investigation and remedial measures, including its adoption of improved anti-corruption and financial reporting programs. Under the terms of the cease and desist order, Westport is required to report to the SEC for a period of two years regarding its improvements to its compliance program and controls.

B. 2018

1. Beam Inc.

Key Facts:

Agencies: SEC
Countries Involved: India
Amount of Total Financial Settlement: $8.2 million
Means of Corruption: Third-party promoters

On July 2, 2018, Beam Inc. (*a.k.a*. Beam Suntory Inc., "Beam") agreed to pay approximately $8.2 million to resolve claims that it violated the books and records and internal controls provisions of the FCPA through the actions of its Indian subsidiary. Without admitting or denying the SEC's allegations, Beam consented to the entry of a cease and desist order ("Order"), which details improper payments by Beam's Indian subsidiary from approximately 2006 through 2012.

Headquartered in Chicago, Illinois, Beam is a beverage and spirits company, most famous for its Jim Beam brand bourbon. During the relevant time period, a class of Beam Inc.'s securities was publicly traded on the New York Stock Exchange. In April 2014, Suntory Holdings Limited acquired Beam Inc. and Beam Inc. delisted from the NYSE. From that point, Beam operated in the name of Beam Suntory Inc. Beam's Indian subsidiary, Beam Global Spirts & Wine (India) Private Limited ("Beam India"), was acquired in 2006. Beam India's books and records were consolidated into that of Beam's and reported by Beam on its financial statements.

Beam India bottled and sold Beam products in India, where the alcoholic beverage industry is subject to heavy government regulations, covering importation of alcoholic products, shipment between bottling facilities and distribution warehouses, label registration, warehouse licensing prior to retail distribution, and sales to retail stores operated by the Indian government. Through third-party promoters, Beam India allegedly made improper payments to government officials to promote the sale of Beam products at government-owned retail stores and to facilitate regulatory processes such as facilities inspection and annual label registration. To conceal the illicit payments, the SEC alleged that third-party promoters issued inflated or fabricated invoices to Beam India, which were falsely characterized in Beam India's books and records as legitimate business expenses such as "Customer Support" or "Off-Trade Promotions."

Beam India also allegedly made payments to government officials to obtain or accelerate registration, inspection, and licensing requirements. For example, in 2011, to accelerate a label application that had been stalled for months, Beam India allegedly paid a senior excise official a total of one million Indian Rupees ($18,000 at the then exchange rate) through a third-party bottler. The third-party bottler allegedly submitted two false invoices in the approximate amount of the payment, for the purpose of "consulting services rendered at the bottling facility."

According to the SEC, beginning in January 2011, Beam began to receive information calling into question the practices of Beam India. A report of a global accounting firm that had been retained to conduct a compliance review of Beam India noted that certain executives of Beam India believed that promoters may be making grease payments to Indian government officials. Over the course of the next year, Beam continued to receive indications of its risks in India, including the July 2011 news of FCPA violations in India by Beam's direct competitor, Diageo

plc, in July 2011. Although Beam took certain steps to address the problems, the SEC alleged that Beam did not take full remedial measures until whistleblower reports and another compliance reports led to an internal investigations in September 2012.

Beam's $8.2 million settlement consists of disgorgement of profit in the amount of $5,264,340, prejudgment interest of $917,498, and a civil monetary penalty of $2,000,000. In reaching the settlement, the SEC noted Beam's failure to timely remediate the deficiencies in its FCPA compliance and internal controls. On the other hand, the SEC acknowledged Beam's voluntary disclosure of the misconduct, cooperation in producing relevant documents and findings, and remedial actions taken in a timely manner following its internal investigation. Beam's remedial measures included ceasing business operations at Beam India until satisfaction of its compliance operation, terminating Beam India employees involved in the misconduct, terminating third-party promoters in India, and enhancing its anti-corruption compliance procedures on a global basis, with an emphasis on third-party due diligence.

Along with Diageo and Anheuser Busch InBev, Beam is at least the third beverage company that has resolved FCPA allegations based, at least in part, on improper payments made to officials involved in the regulation and sale of alcoholic beverages in India.

2. Credit Suisse

Key Facts:

Agencies: SEC
Countries Involved: China, other APAC
Amount of Total Financial Settlement: $76.7 million
Means of Corruption: Hiring

In May and July 2018, Credit Suisse Group AG ("Credit Suisse") and its subsidiary, Credit Suisse (Hong Kong) Limited ("Credit Suisse HK") agreed to pay approximately $76.7 million in penalties and disgorgement to resolve investigations by the DOJ and SEC into Credit Suisse's illicit referral hiring program in the Asia-Pacific region, which, according to the DOJ and SEC, violated the FCPA's internal controls and anti-bribery provisions.

Credit Suisse is a Switzerland-based corporation with numerous subsidiaries, affiliated companies, and branches around the globe. At all relevant times, its shares were publically traded on the New York Stock Exchange, qualifying Credit Suisse as an "issuer" under the FCPA. Credit Suisse HK is a wholly-owned, Hong Kong-registered subsidiary of Credit Suisse that offers securities products and financial advisory services under the Credit Suisse brand in the Asia-Pacific Region. Under the FCPA, Credit Suisse HK constituted an "agent" of issuer Credit Suisse.

a. Referral Hiring Program

The SEC and DOJ alleged that between 2007 and 2013, Credit Suisse HK provided employment to more than 100 relatives and friends referred by or connected to Chinese government officials ("referral hires") in order to obtain or retain investment banking business from Chinese state-owned enterprises and regulatory approvals from government agencies. Senior managers in Hong Kong repeatedly engaged in such practices to improperly influence Chinese government officials in explicit and knowing violation of Credit Suisse's anti-corruption policies against the *quid pro quo* hiring of government officials and their relatives. Credit Suisse HK senior managers designated some referral hires as "must hire" despite the fact that the candidates did not meet Credit Suisse's hiring standards and instructed subordinate employees to inflate the candidates' interview ratings. To track how referral hires' relationships to government officials "translated" into business opportunities, Credit Suisse HK maintained spreadsheets linking each referral hire to the business or approval granted by the related SOE or agency.

The DOJ and SEC outlined numerous instances where Credit Suisse HK managers communicated in emails the need to hire, promote, or compensate otherwise unqualified individuals to secure business. For example, Referral Hire A, the daughter of a high-ranking official at a Chinese SOE ("SOE A"), was hired in 2010 according to instructions from a Credit Suisse HK Vice President and a senior investment banking manager. Referral Hire A was rushed through the hiring process because she was "a princess" and because her hiring would allow Credit Suisse HK to "push her mum" and "get [Credit Suisse HK] in the deal." To accomplish this, Credit Suisse HK employees even created a new resume for her to make her application more presentable. Referral Hire A was hired only six days after Credit Suisse HK received her resume, and the next month, Credit Suisse HK was awarded business by one of SOE A's subsidiaries that earned $950,000 in fees. Until Referral Hire A's resignation in May 2015, Credit Suisse HK regularly promoted Referral Hire A despite her poor performance because of the business awarded to Credit Suisse HK by her mom. In total, Referral Hire A collected more than $1 million in compensation from Credit Suisse HK between 2010 and 2015.

In another example included in the charging documents, Referral Hire B was referred to Credit Suisse HK by Foreign Official B, a high-ranking official at another Chinese SOE. In December 2007, Referral Hire B was offered a three-month internship in Shanghai and, at the request of Foreign Official B, was offered a full-time position in Hong Kong in March 2008. In May 2008, Credit Suisse was selected as the bookrunner for the IPO of the subsidiary of the Chinese SOE and as financial advisor on an M&A transaction for the Chinese SOE. These two mandates earned approximately $21.3 million for Credit Suisse HK. During the 2008 financial crisis, Credit Suisse HK senior managers eliminated highly-rated analysts in favor of keeping Referral Hire B because of the promise of forthcoming "relationship revenue" from Referral Hire B. In March 2009, the Chinese SOE awarded Credit Suisse a mandate that generated $1.18 million in revenue. In several other instances, Credit Suisse's inclusion of Referral Hire B on a deal team or Referral Hire B's personal communications with Foreign Official B were sufficient to secure Credit Suisse a role in an upcoming deal.

b. Resolution of the Allegations

On May 24, 2018, Credit Suisse HK entered into a non-prosecution agreement with the DOJ related to the hiring scheme. Credit Suisse HK and Credit Suisse agreed to pay a $47 million criminal penalty and to continue cooperating with the DOJ in its investigation relating to the conduct. On July 5, 2018, Credit Suisse agreed to pay disgorgement of $24.9 million and $4.8 million in interest to the SEC. The SEC stated that it took the criminal penalty from the DOJ into consideration in deciding that it would not impose any civil penalties. While the DOJ did not require the appointment of a compliance monitor, Credit Suisse HK and Credit Suisse agreed to report at least once every 12 months over a period of three years regarding ongoing remediation efforts and the implementation of a strengthened compliance program at Credit Suisse HK and Credit Suisse.

The criminal penalty against Credit Suisse HK represented a 15% discount off the low end of the U.S. Sentencing Guidelines fine range. Credit Suisse HK received credit for its (and Credit Suisse's) cooperation with the DOJ's investigation, including voluntarily making foreign-based employees available for interviews in the U.S. and providing translations of foreign language documents. The DOJ did not award the full 25% reduction to which Credit Suisse HK may have been eligible because, according to the DOJ, Credit Suisse HK failed to sufficiently discipline employees who engaged in the misconduct.

3. Dun & Bradstreet

Key Facts:

Agencies: SEC
Countries Involved: China
Amount of Total Financial Settlement: $9.2 million
Means of Corruption: Joint ventures, third-party agents, cash

On April 23, 2018, the SEC filed a cease and desist order against Dun & Bradstreet Corporation (“D&B”) for alleged violations of the FCPA’s accounting and internal controls provisions. D&B, a publicly-traded Delaware company based in New Jersey, is a global provider of business information, and it conducts reporting of credit and commercial data on millions of companies. According to the SEC, from 2006 to 2012, two of D&B’s indirect subsidiaries in China, Shanghai Huaxia Dun & Bradstreet Business Information Consulting Co., Limited (“HDBC”) and Shanghai Roadway D&B Marketing Services Co., Ltd. (“Roadway”), made improper payments to government officials and Chinese SOEs in order to obtain or retain business.

Without admitting or denying the SEC’s allegations, D&B agreed to disgorge profits of $6,077,820 and pay $1,143,664 in prejudgment interest. Additionally, D&B agreed to pay a civil penalty in the amount of $2 million.

The DOJ issued D&B a formal declination under the FCPA Corporate Enforcement Policy.

a. Alleged Misconduct

i. HDBC Joint Venture

In 2006, through D&B’s Chinese subsidiary, Dun & Bradstreet International Consultant (Shanghai) Co. Ltd. (“D&B China”), D&B formed the joint venture HDBC with Huaxia International Credit Consulting Co. Limited (“Huaxia”). D&B China owns 51% of HDBC.

According to the SEC, D&B performed due diligence on Huaxia before the formation of HDBC, which revealed that Huaxia relied on its government connections to source non-public and restricted information directly from various government agencies, including the State Administration of Industry and Commerce. While D&B’s senior managers were reportedly aware that Huaxia routinely made improper payments to government officials in exchange for information, D&B failed to adequately address the issue. Instead, D&B merely provided a short FCPA training to Huaxia executives and requested that they complete anti-bribery questionnaires and certifications.

The SEC further alleged that after HDBC was established, D&B stopped Huaxia employees’ practice of making direct payments to Chinese government officials in exchange for confidential information and began using third-party agents to achieve the same goal. D&B reportedly took this approach under the mistaken belief that using third parties would shield the company from legal liability, and the tactic made data acquisition costs in China significantly higher than similar costs in other countries. In 2008, D&B considered eliminating the use of third parties and instructing HDBC employees to purchase data directly from government officials. However, employees responsible for data and operations at HDBC allegedly reported that direct purchases would require “lots of palm grease.” The Order alleges that D&B was also concerned that it could not obtain tax receipts if it purchased information directly from officials. In the end, D&B allegedly opted to continue using third parties to provide illicit payments to government officials in order to gain advantages for HDBC, a practice that did not end until 2012.

ii. Roadway

Roadway was a direct marketing services company in China that purchased much of its data from third-party vendors. In June 2009, D&B acquired 90% of Roadway through a wholly owned subsidiary. D&B reportedly conducted pre-acquisition due diligence on Roadway. During this due diligence, Roadway reportedly refused to warrant that its sales force did not pay kickbacks to decision-makers to “drum up” business. Despite this clear red flag, D&B allegedly failed to further investigate whether Roadway acquired its data by any illegal means, or whether the company’s sales force was paying bribes to government officials.

After the acquisition, Roadway continued its practice of purchasing consumer data from third parties. D&B was satisfied with certifications from those third parties stating that the data was legally obtained, although D&B allegedly did not audit or review the sources of the data purchased, or otherwise verify whether the data was obtained legally.

D&B also allegedly failed to verify whether Roadway employees were making improper payments to customer decision-makers. According to the SEC, from July 2009 to March 2012, Roadway employees made improper payments disguised as “promotional expenses” to customers in order to obtain or retain business, including payments to Chinese government agencies and SOEs. These “promotional expenses” were provided to customers both through agents and by Roadway employees directly. During the relevant period, 34% percent of customer transactions involved such “promotional expenses,” which covered over a thousand customers, including 156 Chinese government agencies and SOEs.

On March 15, 2012—China’s National Consumer Protection Day—a Chinese news program revealed the existence of Roadway’s extensive databases of citizen information, which included “specific financial, employment, and contact information that Roadway sold to companies for marketing purposes.” Police in Shanghai raided Roadway’s headquarters the same day, confiscating electronic databases and detaining individuals involved with Roadway’s data acquisition operations. In September 2012, the Chinese government charged Roadway with illegally obtaining private information of citizens and ordered the company to pay a $160,000 criminal fine.

b. Resolution

The Order states that illicit payments by HDBC and Roadway were falsely recorded as legitimate business expenses, which were consolidated in D&B’s books and records. Furthermore, the Order alleges that despite concerns raised during pre-transaction due diligence, D&B failed for several years to develop and maintain a sufficient system of internal controls to prevent and detect improper payments in data acquisitions and sales. The SEC consequently charged D&B with violations of the FCPA’s accounting and internal control provisions.

On April 23, 2018, the DOJ issued D&B a formal declination under the FCPA Corporate Enforcement Policy. The DOJ stated that it had reached this decision “despite the bribery committed by employees of the [c]ompany’s subsidiaries in China” based on a number of factors. These included: prompt and voluntary self-disclosure; thorough internal investigation; full cooperation with authorities, including identifying responsible individuals, providing the DOJ with all relevant facts, making both current and former employees available for interviews, and translating documents to English as necessary; full remediation, including terminating 11 employees involved in the misconduct and disciplining others with financial sanctions and formal reprimands; and agreement to disgorge the improper profits in full to the SEC.

4. Elbit Imaging Limited

Key Facts:

Agencies: SEC
Countries Involved: Romania, U.S.
Amount of Total Financial Settlement: $500,000
Means of Corruption: Third-party consultants, sales agents

On March 9, 2018, the SEC filed a cease and desist order against Elbit Imaging Ltd. ("Elbit") related to its findings that Elbit had violated the FCPA's books and records and internal accounting controls provisions in real estate projects in both Romania and the United States. According to the SEC, Elbit and its subsidiary, Plaza Centers NV ("Plaza"), made payments to two third-party consultants and a sales agent without evidence that these third parties provided actual services. Elbit consented to the order without admitting or denying the SEC's findings and agreed to pay a $500,000 civil penalty in order to settle the FCPA violations.

Elbit is headquartered in Petach Tikva, Israel. An international holding company, Elbit owns subsidiaries in various industries, including real estate development. Plaza is a Netherlands corporate entity that focuses on constructing and modernizing "Western-style" shopping and entertainment centers in Central and Eastern Europe. Plaza was at the time of the relevant conduct majority-owned and controlled by Elbit and its financial statements were consolidated into Elbit's financial statements.

Until February 2014, Elbit's then-CEO, Mordechai (Moti) Zisser, held majority ownership in Elbit. Moti Zisser also served as Plaza's Executive Director until February 2014.

a. Casa Radio Project

In 2006, Plaza sought to participate in the Casa Radio Project, a large real estate development project located in Bucharest, Romania. Plaza engaged two third-party consultants, one in 2006 (the "2006 Consultant") and one in 2011 (the "2011 Consultant"). Both consultants were offshore entities allegedly retained at Mr. Zisser's direction. The SEC found no evidence to suggest that Plaza conducted any pre-engagement due diligence on either consultant.

The 2006 Consultant was nominally hired to, among other tasks, provide consulting services and assistance in obtaining government approvals for the development project. In February 2007, Plaza purchased a 75% interest in the Casa Radio Project for $40 million and a commitment to finance and develop a Romanian public authority building. The SEC found no evidence that the 2006 Consultant provided any services in connection to this transaction.

The 2011 Consultant was similarly hired to assist Plaza in securing governmental approvals and to assist Plaza in purchasing from the Romanian government an additional 15% interest in the Casa Radio Project. Although Plaza successfully acquired the 15% interest in the project, the SEC found no evidence that the 2011 Consultant had provided any services in relation to this acquisition.

In total, Plaza, directly or indirectly, paid the 2006 and 2011 Consultants approximately $14 million from 2007 through 2012. Plaza senior officers authorized these payments despite the absence of requisite documentation to support the payments. Additionally, Plaza categorized these expenses in its books as legitimate business expenses for services rendered. In its findings, the SEC alleged that some or all of the funds may have been used to make corrupt payments to Romanian officials or were simply embezzled.

b. U.S. Real Estate Portfolio Sale

In late 2011, a joint venture of investors (the “Joint Venture”), of which Elbit and Plaza together held a 45.4 percent stake, sought to sell a portfolio of 47 shopping center real estate assets in the United States (the “Portfolio”). The Joint Venture hired a financial advisor (the “JV advisor”) to assist the Joint Venture in selling these assets. The JV advisor ultimately received $6.75 million for services rendered in relation to the June 2012 sale of the Portfolio.

In November 2011, approximately six weeks after the Joint Venture retained the JV advisor, Elbit and Plaza entered into a sales agency agreement with an offshore entity (“Sales Agent A”), for the stated purpose of assisting Elbit and Plaza in selling the Portfolio. Sales Agent A was not hired by the Joint Venture and Elbit and Plaza did not conduct any due diligence on Sales Agent A. Under Sales Agent A’s contract with Elbit and Plaza, Sales Agent A was responsible for creating marketing materials, locating potential buyers, and assisting in negotiating a sales contract, services which largely mirrored those for which the JV advisor had already been retained. In exchange, Sales Agent A would receive a success fee totaling 0.9% of the Portfolio’s gross sale price.

The day after Elbit and Plaza executed the sales contract with Sales Agent A, Sales Agent A subcontracted with another offshore entity (“Sales Agent B”), assigning all of its rights and responsibilities under the Sales Agent Agreement to the second entity. Mr. Zisser indirectly owned Sales Agent B, which was to receive approximately 98% of remuneration due to Sales Agent A under this subcontract. Mr. Zisser did not disclose his interest in Sales Agent B, and Elbit and Plaza were not aware that Sales Agent A had subcontracted with this entity.

The Joint Venture sold the Portfolio on June 21, 2012, for $1.428 billion. Following the sale, Elbit and Plaza paid Sales Agent A $13 million, or almost double the commission paid to the JV advisor. The $13 million was nominally for Sales Agent A’s commission and expenses and was paid despite the absence of requisite proofs of services rendered. Sales Agent A in turn paid Sales Agent B $12.75 million. Only Mr. Zisser was aware of this remuneration scheme. In its investigation of these payments, the SEC did not identify any evidence showing that either Sales Agent A or Sales Agent B had provided services related to this agreement.

c. Resolution

Elbit and Plaza self-reported to the Romanian and U.S. authorities following Elbit’s discovery of information suggesting that payments made by Plaza in relation to the Casa Radio Project may have been improper and incorrectly recorded in Plaza’s books and records. Elbit, through a special committee of its board of directors, retained outside counsel to conduct an independent investigation. While the investigation was being conducted, additional information came to light regarding Elbit and Plaza’s payments to Sales Agent A and Sales Agent B’s ownership. This new information led Elbit and Plaza to form a joint special committee to review the Portfolio sale. Elbit shared its external counsel’s findings with the SEC, including providing translations of certain documents, and was responsive to the SEC’s requests for additional information.

The SEC determined that Elbit and Plaza’s internal accounting controls failed to identify that payments of $27 million were made to the 2006 Consultant, 2011 Consultant, and Sales Agent A with little or no indication that these parties had actually provided services justifying this remuneration. The SEC noted in particular that Plaza’s legal department had limited involvement in, and oversight over, Plaza’s contracts with third-party agents and consultants. These deficiencies in Plaza’s internal controls led to inaccuracies in Elbit’s books and records. Finally, neither Elbit nor Plaza maintained policies and procedures aimed at detecting corruption risks or training employees on anti-corruption compliance. In agreeing to the settlement, the SEC positively cited Elbit and Plaza’s self-reporting to the authorities, implementation of “extensive” remedial measures, and full cooperation with the

SEC investigation alongside a thorough internal investigation. It additionally noted that Elbit was in the process of selling its principal assets in order to service its debt obligations and was not developing current or new business.

5. Eletrobras

Key Facts:

Agencies: SEC
Countries Involved: Brazil
Amount of Total Financial Settlement: $2.5 million
Means of Corruption: Inflated construction costs

On December 26, 2018, Centrais Elétricas Brasileiras S.A. (“Eletrobras”), a Brazilian power generation, transmission, and distribution company, consented to the entry of an administrative cease and desist order and agreed to pay a $2.5 million civil penalty in connection with a settlement with the SEC relating to alleged violations of the FCPA’s internal accounting controls and recordkeeping provisions.

Between 2009 and 2015, Eletrobras Termonuclear S.A. (“Eletronuclear”), an Electrobras majority owned (99%) subsidiary, renegotiated and executed two contracts, then valued at approximately $4.6 billion and $1.1 billion, relating to construction of a new nuclear power plant (“UTN Angra III”). According to the SEC, executives at unspecified construction companies inflated the costs of various projects in connection with the contracts and used the overpayments to fund bribes to the high-level officials at Eletronuclear and individuals associated with two of Brazil’s largest political parties. Pursuant to the scheme, construction company executives allegedly agreed to pay 2 percent of the contract value to officials associated with two of Brazil’s largest political parties, approximately $4.1 million to the former Eletronuclear president, and approximately $4.9 million to other former Eletronuclear officers. In return, the former Eletronuclear officers used their influence over the contract’s prequalification, budgeting, and procurement processes to authorize unnecessary contractors and create sham invoices that inflated the cost of Eletronuclear’s infrastructure project.

The SEC alleged that the former Eletronuclear officers caused Eletronuclear to approve and pay invoices from contractors involved in the bid-rigging and bribery scheme. According to the SEC, Electronuclear paid at least 28 invoices from a contractor used as a conduit for the bribes paid to the former Eletronuclear president. Eletronuclear recorded these inflated contract prices and sham invoices as legitimate expenses for goods or services in connection with UTN Angra III and consolidated those expenses to Eletrobras. As such, Eletrobras’s books and records did not, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the company’s assets. According to the SEC, Eletrobras violated the books and records and internal controls provisions by maintaining insufficient internal accounting controls and by recording as legitimate expenses the payment of sham invoices used to inflate contracts.

The SEC indicated that Eletrobras’s anticorruption policies and accounting controls were insufficient because they often did not apply to all employees or were ignored. For example, its code of ethics initially applied only to Electrobras and not to its 13 regional subsidiaries or 175 special purpose entities, where the majority of its employees worked. Eletrobras’s ethical principles required the selection and hiring of suppliers based on specific criteria, but these criteria, including criteria requiring payments to suppliers be proportional to the worked performed, were frequently ignored or circumvented, in part because Eletrobras lacked internal control over financial reporting.

In agreeing to the settlement terms, the SEC considered remedial acts and cooperation by Eletrobras in its investigation. Eletrobras cooperated by sharing facts of its internal investigation and by voluntarily producing and translating documents. Electrobras also pursued remedial action by disciplining employees involved in the misconduct, enhancing its internal accounting controls and compliance functions, remediating material

weaknesses identified in its annual reports with the SEC, and adopting new anti-corruption policies and procedures.

6. Raul Gorrin Belisario

Key Facts:

Agencies: DOJ
Countries Involved: Venezuela
Means of Corruption: Cash payments using offshore accounts and shell companies, gifts of luxury items

On August 16, 2018, Raul Gorrin Belisario ("Gorrin"), a Venezuelan billionaire, trained lawyer, and media mogul, was charged in the Southern District of Florida with one count of conspiracy to violate the FCPA, one count of conspiracy to commit money laundering, and nine counts of money laundering. On November 19, 2018, the U.S. District Court for the Southern District of Florida unsealed an indictment against Gorrin for bribery- and money laundering-related offenses. Gorrin's indictment is linked to the guilty pleas (in December 2017 and March 2018 respectively) of two other high-profile Venezuelan nationals, Alejandro Andrade Cedeno (hereinafter "Andrade") and Gabriel Arturo Jimenez Aray (hereinafter "Jimenez") – both of whom admitted to receiving bribes from and conspiring with Gorrin. In November 2018, Andrade was sentenced to 10 years in prison and Jimenez to three years.

The bulk of the bribes allegedly paid by Gorrin were made to Andrade, who the unsealed indictment refers to as "Foreign Official 1" serving as a high level official with decision-making authority and influence within the Venezuelan National Treasury ("ONT"). According to the indictment, in 2008, Gorrin offered to enter into a scheme with Andrade, whereby Gorrin would pay Andrade bribes in exchange for Andrade facilitating Gorrin's involvement in "foreign exchange transactions at favorable rates for the Venezuelan government." Andrade also gave Gorrin the access and influence necessary to "obtain and retain contracts" with the ONT. The bribe payments to Andrade continued after he left ONT in 2010. Notably, Gorrin allegedly paid more than $94 million to Andrade between 2011 and 2017 to guarantee Andrade's silence and compliance with Gorrin's foreign exchange scheme and for having secured an introduction to "Foreign Official 2" (a second high-level official within the ONT). Gorrin allegedly continued the foreign exchange scheme with Foreign Official 2, following Andrade's departure. According to the DOJ, the bribe payments to "Foreign Official 2" amounted to more than $65 million between 2011 and 2013.

To pay Andrade and Foreign Official 2, Gorrin allegedly used his personal Swiss bank account, as well as bank accounts held by entities that he owned or controlled, identified as "Company 1," "Company 2," and "Company 3" in the indictment. According to the DOJ, these companies were nothing more than shell companies. Many of the alleged payments originated from bank accounts in Switzerland and were deposited into accounts located in Florida and New York.

In addition to payments by wire transfer, Gorrin allegedly purchased (and covered expenses related to) luxury items and property for Andrade and "Foreign Official 2." For example, Andrade allegedly received three jets, a yacht, show-jumping horses, and designer watches from Gorrin. "Foreign Official 2" and his spouse also received jets and a yacht.

In addition to the bribery scheme and related foreign exchange scheme, Gorrin also allegedly approached Jimenez (identified as "Foreign Bank Official" in the DOJ's indictment) in 2010. At the time, Jimenez (a Venezuelan national) owned Banco Peravia, a bank based in the Dominican Republic. Gorrin partnered with Jimenez to acquire Banco Peravia, with the alleged goal of using the bank to launder bribe payments to

Venezuelan officials (including payments made to Andrade and “Foreign Official 2”), as well as to launder the proceeds of this and other schemes.

7. Patrick C.P. Ho

Key Facts:

Agencies: DOJ
Countries Involved: Uganda; Chad
Means of Corruption: Cash, political contributions, charitable donations

In December 2018, following a one-week jury trial before U.S. District Judge Loretta A. Preska in the Southern District of New York, Chi Ping Patrick Ho, a.k.a. Patrick C.P. Ho a.k.a. He Zhiping (“Ho”) was convicted of conspiring to violate the FCPA, violating the FCPA, conspiring to commit international money laundering, and committing international money laundering. The charges against Ho, initially unsealed in a criminal complaint in November 2017, relate to his work as the Deputy Chairman and Secretary-General of the China Energy Fund Committee (“CEFC”). In March 2019, Ho was sentenced to three years of imprisonment and $400,000 in fines.

Initially, Ho was charged alongside Cheikh Gadio, the former Senegalese Minister of Foreign Affairs (from approximately 2002 to 2009). However, in September 2018, the DOJ requested that the charges against Gadio be dismissed. At the same time, Gadio’s attorneys indicated that Gadio was looking forward to continuing his cooperation with U.S. authorities.

According to the complaint and the findings at trial, Ho and Gadio orchestrated a scheme to bribe officials at the highest levels of the Ugandan and Chadian governments for the benefit of CEFC, a Chinese oil and gas conglomerate. Ho and Gadio conspired to bribe African government officials, including Chadian President Idriss Déby, to secure oil rights and other business benefits for CEFC. The charges focused on two separate conspiracies, one targeting Chad and the other targeting Uganda. Both conspiracies initiated in the halls of the United Nations while Sam Kutesa, who later became the Foreign Minister of Uganda, served as President of the General Assembly. Both the Chad and Uganda conspiracies lasted from at least in or about late 2014 through January 2017.

CEFC is headquartered in Shanghai, with $39 billion in revenue in 2015 and affiliates worldwide, including in New York. CEFC funds an NGO for which Ho served as the Secretary-General and Deputy Chairman. The NGO is based in both Hong Kong and the United States and held or holds Special Consultative Status with the UN Economic and Social Council. The NGO’s Special Consultative Status afforded Ho access to meetings with UN officials that are not open to general members of the public. Prosecutors asserted jurisdiction over Ho on the basis that he was an agent of a domestic concern and that he took actions in furtherance of the scheme while in the United States.

a. Chadian Scheme

The first scheme began sometime around September or October 2014. Ho sought the assistance of Gadio, who had a personal relationship with President Déby of Chad. CEFC wished to enter into a joint venture with a Chinese government-owned oil and gas company, now understood to be China National Petroleum Corporation (CNPC), but that company was facing substantial legal hurdles. At the time, Chad had fined CNPC $1.2 billion for environmental violations and revoked its oil licenses. At Ho’s direct request, Gadio met with the President Déby in October 2014 and conveyed Ho’s offer to provide, in Gadio’s words, “financial assistance for [the President’s] political campaigns” in exchange for reconsideration of the decision to revoke CNPC’s licenses. Although Chad ultimately entered into a settlement with CNPC, the desired joint venture between CNPC and CEFC never materialized. As a result, Ho tried other tactics to secure oil rights for CEFC in Chad. In November 2014, Gadio

arranged a face-to-face meeting between Ho and President Déby in New York, where they discussed potentially lucrative oil rights available in Chad. In December 2014, Ho and a group of CEFC China executives flew to Chad on a corporate jet with $2 million in cash concealed in gift boxes to present to President Deby as a bribe in return for access to these oil rights. President Déby rejected the bribe offer. According to Gadio's testimony during Ho's trial, President Déby was enraged at the offer. President Déby later agreed to accept the money as a charitable donation to the country, and Ho and his CEFC China colleagues created a paper trail to suggest that it was always intended as such.

According to prosecutors, CEFC was given preferential treatment and offered certain oil rights without competition. However, CEFC instead purchased other oil rights from a Taiwanese company.

b. Ugandan Scheme

Shortly after Sam Kutesa began his term as President of the 69th Session of the UN General Assembly ("PGA"), Ho sought to cultivate a relationship with Kutesa with the intent to ultimately connect with the President of Uganda. Kutesa, who otherwise served as the Foreigner Minister of Uganda when not in the position of PGA, is related to the President of Uganda, Yoweri Museveni. During his time as PGA, Kutesa frequently met with Ho to discuss CEFC and the prospect of forming a "strategic partnership" between Uganda and CEFC once Kutesa returned to Uganda. In August 2015, during a trip to China, Kutesa appointed the Chairman of CEFC, Ye Jianming, as a "Special Honorary Advisor." News reports at the time indicate that Chairman Ye emphasized CEFC's interest in deepening its cooperation with Uganda, while Kutesa suggested that he would support CEFC's investment in the energy and financial sectors in Uganda and other African countries. During this trip, Kutesa obtained a promise that CEFC would provide a "donation" to support Museveni's reelection campaign.

Once Museveni was reelected president and Kutesa had returned to Uganda, Kutesa solicited the $500,000 "contribution" he had previously requested. The money was described by Kutesa and others in various communications as either for the benefit of the president's reelection campaign (which had already been concluded) or as a "donation" to "support" Kutesa. In early May 2016, Ho wired $500,000 dollars from Hong Kong through New York to a Ugandan bank account controlled by a Ugandan foundation designated by Kutesa.

Ho and CEFC executives attended Museveni's inauguration and met with Museveni and top Ugandan officials, including with the Department of Energy and Mineral Resources. After the trip, Ho requested that Kutesa and Museveni assist CEFC to acquire a Ugandan bank, so it could pursue more business opportunities in Uganda. Ho also offered to "partner" with Kutesa and Museveni and/or their "family businesses," making clear that both officials would be able to benefit from CEFC's business dealings. In exchange for the bribes paid by Ho, Kutesa steered a bank acquisition opportunity to CEFC.

8. Kinross Gold

Key Facts:

Agencies: SEC
Countries Involved: Mauritania; Ghana
Amount of Total Financial Settlement: $950,000
Means of Corruption: Petty cash, vendors/procurement, third party consultant

On March 26, 2018, the SEC entered a cease and desist order against Kinross Gold Corp. ("Kinross"), a NYSE-listed gold mining company based in Toronto, to settle allegations that Kinross violated the FCPA's books and records and internal controls provisions. Without admitting or denying the allegations, Kinross agreed to a yearlong reporting of its remedial steps and a $950,000 civil penalty for failing to devise and maintain proper internal accounting controls post-acquisition of two mining operations in Africa, despite identifying accounting and compliance failures during the pre-acquisition stage.

On November 7, 2017, the DOJ informed Kinross that it was declining to prosecute the same conduct.

According to the SEC, in September 2010, Kinross acquired two African mining operations and associated assets: Tasiast Mauritanie Limited S.A. (“Tasiast”) in Mauritania and Chirano Gold Mines Ltd. (“Chirano”) in Ghana, from Vancouver-based Red Back Mining, Inc. (“Red Back”), for $7.1 billion. During pre-acquisition due diligence, Red Back disclosed its lack of anti-corruption and internal accounting controls surrounding its contractual, procurement, petty cash, and vendor payment processes. Following the acquisition, Kinross failed to timely implement sufficient internal accounting controls and remediate known issues, including the use of petty cash by low-level employees to pay vendors and the lack of due diligence on vendors.

In April 2011, Kinross’ internal audit reported that the accounting and disbursement (Enterprise Resource Planning (“ERP”)) systems at both mining operations contained insufficient details on the nature of disbursements, making it “not possible” to identify suspect payments such as excessive rebates and discounts, advance payments, government commissions, and unjustified business expenses. In addition, internal audit also found that the two mines did not maintain proper tendering and contracting processes. Kinross management, however, failed to remediate these issues. In 2012, at the request of Kinross’ increasingly concerned finance department, another internal audit was conducted, reaching nearly identical conclusions. For example, at both mines, purchase orders were created after invoices were received or were not created at all. Additionally, disbursements were made without required signatures, or the signatures failed to indicate the names and positions of approval for verification purposes.

According to the SEC, Kinross management once again failed to take sufficient remedial action. As a result, from 2012 to 2015, the mines made various questionable payments. For example, between 2012 and 2014, a government customs officer was paid for weeks of fixed travel expenses, although he did not travel. Also in 2012, after Kinross’ mining permit was delayed, a third-party consultant’s $12,000 fee was paid using petty cash for services purportedly provided a year earlier pursuant to an oral contract between Kinross and the consultant. The permit was approved a month after the payment was made. The SEC alleged that Kinross failed to fairly describe these transactions in its books and records.

In 2013, Kinross enhanced its accounting and compliance controls for procurement and payments; however, Kinross failed to maintain these controls, according to the SEC. For example, in 2014, Kinross awarded a $50 million logistical support contract to a less-qualified shipping company with ties to a Mauritanian government official, over a more technically qualified, cheaper competitor. Additionally, Kinross retained and paid $715,000 to a politically exposed consultant without conducting proper enhanced due diligence as required by Kinross’s supply chain policy. The SEC also noted that Kinross did not provide adequate anti-corruption training to its senior management.

In determining the appropriate resolution, the SEC recognized Kinross’ efforts to address its internal accounting and compliances failures, such as conducting additional internal audits, implementing a new ERP system, replacing personnel at both mines, expanding the compliance team, updating relevant policies, conducting compliance training, and instituting formalized procedures to track the use of petty cash. Kinross also agreed to terminate all long-standing agreements with third-party consultants to obtain visas and permits.

9. Koolman and Parker

Key Facts:

Agencies: DOJ
Countries Involved: Aruba
Means of Corruption: Cash
Notes: Scheme was initially revealed through the *Panama Papers* release in 2016, which outed Koolman's offshore accounts

In April 2018, Egbert Yvan Ferdinand Koolman, a Dutch citizen residing in Miami who had served until 2016 as product manager for the Aruban state-owned telecommunications provider, Servicio di Telecommunicacion di Aruba N.V. ("Setar"), pleaded guilty to one count of conspiracy to commit money laundering in connection with funds he derived through a corrupt scheme with Florida businessman Lawrence Parker. Parker previously pleaded guilty to one count of conspiracy to violate the FCPA and to commit wire fraud related payments that he made to Koolman to earn business from Setar.

According to admissions by the two men, from November 2005 to March 2015, Parker made corrupt promises and payments to Koolman in exchange for Koolman's assistance in winning and retaining Setar telecommunications contracts for five phone companies in which Parker held an interest. Parker was a U.S. citizen residing in Miami-Dade County and all five companies were organized under the laws of, and maintained their primary places of business in, Florida. The payments were made in cash to Koolman and his ex-wife and by wire from U.S. bank accounts owned by the Parker's phone companies to foreign bank accounts owned and controlled by Koolman.

In at least two instances, Parker drew a check in his own name from an account owned by one of his phone companies and paid the amount drawn in cash to Koolman. Koolman additionally drew money from a U.S.-based bank account using a bankcard in Aruba. All told, Koolman received over $1.3 million in corrupt payments from Parker and others and drove a reported $23.8 million orders to Parker's companies.

During the relevant period, Koolman's responsibilities included interacting with vendors and purchasing mobile phones and other mobile equipment for Setar. In this position, Koolman was able to favor Parker's companies for lucrative mobile phone and accessories contracts. In addition, Koolman was able to provide Parker with Setar's confidential business information, including competing suppliers' bid information. The DOJ noted at least two instances in which Koolman sent emails with confidential competitor information to Parker's U.S.-based email account.

According to news reports, Koolman was exposed in 2016 when the Panama Papers revealed that Koolman had set up an anonymous offshore entity in the British Virgin Islands and used the company to open two bank accounts in Panama. Following an internal audit, Setar fired Koolman. In March 2017, Setar filed a civil complaint in the U.S. against Koolman, Parker and other entities and individuals.

In June 2018, Koolman was sentenced in the U.S. District Court for the Southern District of Florida to 36 months in prison and was required to pay over $1.3 million in restitution. Koolman will additionally be required to surrender himself to U.S. immigration authorities for removal following his term of imprisonment.

In April 2018, Parker was sentenced in the Southern District of Florida to 35 months in prison and was ordered to pay $701,750 in restitution. U.S. prosecutors recommended a 33% downward departure from the Sentencing Guidelines range for Mr. Parker on the basis of his substantial assistance in the prosecution of other members of the Setar conspiracy, including Koolman.

10. Panasonic

Key Facts:

Agencies: DOJ; SEC
Countries Involved: Middle East, U.S.
Amount of Total Financial Settlement: $280 million
Means of Corruption: Third-party agents, hiring former government officials

On April 30, 2018, Panasonic Corporation ("Panasonic") agreed to disgorge $126.9 million in profits and to pay $16.2 million in prejudgment interest to resolve charges with the SEC that it violated the anti-bribery, books and records, and internal controls provisions of the FCPA as well as other provisions of the Securities Exchange Act of 1934. Panasonic is a multinational electronics corporation headquartered in Japan. Its shares were traded on the New York Stock Exchange as ADRs until April 22, 2013. As a result, Panasonic was an "issuer" within the meaning of the FCPA until that time.

On the same day, Panasonic's wholly-owned subsidiary, Panasonic Avionics Corporation ("PAC"), entered into a deferred prosecution agreement with the DOJ and agreed to pay $137.4 million in criminal penalties to resolves charges that it violated the accounting provisions of the FCPA. PAC was also required to retain an independent corporate compliance monitor for a two-year term. PAC is a wholly-owned subsidiary of Panasonic. PAC designs in-flight entertainment systems and global communication systems for airlines and airplane manufacturers. PAC is headquartered in California and was therefore, at all times, a "domestic concern" under the FCPA.

In total, Panasonic and PAC paid over $280 million as a result of the misconduct described below.

a. Relevant Conduct

From 2007 to 2013, PAC used pass-through entities to make improper payments to third parties that maintained influence over contracts for which PAC was bidding. The funds for these payments originated in the Office of the President Budget, an account over which a single PAC senior executive had sole control and which was subject to very little financial oversight. Despite a 2010 internal audit report circulated to PAC executives stating the risks and potential FCPA violations associated with these practices, payments continued for several more years without interference.

According to the SEC, beginning in 1986, PAC engaged a sales representative ("Sales Representative") in the Middle East to assist with sales and contract negotiations of its products in the region. Despite having no background in avionics and warning from PAC employees on the ground that Sales Representative was paying bribes to win business for PAC, Sales Representative received more than $184 million in commissions from PAC between 2007 and 2016 through his British Virgin Islands-based corporate entity. During this time, Sales Representative presented himself as a direct employee of PAC, using PAC-branded business cards that listed him as PAC's General Manager of Sales and Marketing in the Middle East, Africa, and South Asia; maintaining an office in PAC's Dubai office; and conducting business through a PAC phone number and email address.

In 2004, PAC and a state-owned airline in the Middle East signed a Master Product Supply Agreement ("MPSA") valid for ten years. The airline appointed an executive ("Foreign Official") to serve as the primary point of contact for negotiations with PAC, and in 2006, PAC and Foreign Official began negotiations on an Amendment to the MPSA ("Amendment One"). According to the SEC, during the course of these negotiations, Foreign Official sought and obtained assistance from Sales Representative in obtaining clients for a private consulting business he had recently started.

In 2007, PAC and Foreign Official began negotiating a second amendment to the MPSA ("Amendment Two"). At the same time, Foreign Official began to solicit a high-paying position with PAC from Sales Representative.

According to the SEC, as discussions regarding Foreign Official's eventual employment with PAC progressed, Foreign Official provided PAC with confidential information, advice on negotiating additional business with the Middle East airline, and tips for maintaining the relationship with the airline. In September 2007, PAC offered Foreign Official a position as a PAC Consultant with annual remuneration of $200,000 plus travel expenses. Amendment Two was signed in November 2007, and, in February 2008, Foreign Official resigned from his position at the airline and was retained as a consultant by PAC. PAC disguised its consultancy relationship with Foreign Official by arranging for a separate third party to formally retain Foreign Official as a consultant and to pass through payments to Foreign Official. In this manner, Foreign Official was paid $875,000 between 2008 and 2014 from the Office of the President Budget in exchange for no demonstrable services. These payments to Foreign Official were falsely recorded in PAC's books as consulting expenses and later improperly recorded as "selling and general administrative expenses" in Panasonic's books. Between April 2007 and March 2012, PAC earned $92.8 million in profits from the Middle East airline through programs that Foreign Official had some involvement with or influence over.

Similarly, in October 2007, PAC retained as a consultant a former PAC employee who had also been hired as a consultant by one of PAC's largest domestic customers. From October 2007 to December 2013, the consultant was retained by both PAC and the customer. During this time, the consultant repeatedly provided confidential, non-public business information to PAC and used his ability and influence with the customer. Beyond providing inside and confidential information to PAC, the consultant provided few services to PAC. PAC paid the consultant a total of $825,000 from October 2007 to December 2013. PAC employees disguised payments to the consultant by using a third party as a pass-through. Compensation was improperly recorded as "consultant payments" without sufficient documentation to substantiate the nature of the payments and were ultimately improperly recorded as "selling and general administrative expenses" on Panasonic's books. PAC earned approximately $22.6 million in profits from programs that the consultant had influence over in his role as an employee for the customer.

In 2009, PAC implemented a formal review process for new and existing sales agents. The procedure required PAC employees to collect basic information regarding sales agents and for each sales agent to obtain a certification from TRACE International, a third-party non-profit organization that conducts due diligence reviews, prior to engagement by PAC. An Internal Review Committee ("IRC") then reviewed and provided final approval for each proposed sales agent. However, PAC employees subverted this process by engaging sales agents that had failed to sign the anti-bribery certification. They engaged these sales agents as sub-contractors of a certified sales agent. Between 2008 and April 2013, PAC employees directed more than $7 million to 13 uncertified sub-agents disguised as commission payments to a single certified Malaysian sales agent who then passed on payment to the sub-agents for a 1-2% fee.

The SEC noted that the implemented due diligence procedures were ineffective. The SEC stated that the IRC never rejected a proposed sales agent and made judgments based only on a single-page form containing cursory information regarding proposed sales agents, not any of the due diligence documentation. Furthermore, the IRC did not question the decline in the number of agents used after due diligence requirements were implemented, nor did it take issue with the ability of one Malaysian sales agent to perform work on approximately fifty sales campaigns with twenty airlines. Likewise, PAC compliance personnel did not possess sufficient qualifications or training and failed to respond to clear red flags such as a referral by the state-owned airline customer. As a result, the SEC found that Panasonic failed to devise and maintain a sufficient system of internal controls in connection with the retention of sales agents.

In 2010, a senior finance executive at PAC requested that PAC's Internal Audit Department conduct an audit of the company's vendor selection, payment processing, and contract execution. The resulting audit report identified numerous compliance risks stemming from PAC's use of a particular third party to retain and pay consultants. Although the audit report was circulated among PAC executives in various forms from September 2010 through November 2012, PAC took no significant actions to address the issues raised and the suspect payments continued during this period.

b. Penalty

PAC did not receive voluntary disclosure credit because it did not voluntarily disclose the activity even after learning of and investigating the allegations as the result of a whistleblower complaint and civil suit. PAC's disclosure came only after the SEC requested documents from Panasonic related to potential violations of anti-corruption law. However, the DOJ did recommend that PAC receive a twenty percent discount from the low end of the U.S. Sentencing Guidelines fine range for cooperating with the DOJ's investigation. This cooperation included conducting a thorough internal investigation; making factual presentations to the DOJ; sharing facts learned during witness interviews conducted by the company; voluntarily making foreign and U.S. employees available for interview by the DOJ and SEC; alerting the DOJ to material information; collecting, analyzing, and organizing large quantities of evidence from multiple jurisdictions; and disclosing its Middle East misconduct to the DOJ when the government was not previously aware of it. PAC also received credit for significant remedial measures, including terminating several senior executives who were involved in or aware of the misconduct.

c. Individual Prosecutions

On December 18, 2018, the SEC issued settled cease and desist orders against two former PAC executives related to the executives' involvement in the misconduct.

The SEC order against Paul Margis, PAC's former President and CEO, alleged that Margis authorized PAC's retention of and payment to the consultants described above. Margis also allegedly exerted control over the Office of the President Budget from which the funds to pay the consultants derived. Margis neither admitted nor denied the findings of the SEC order. He agreed to pay a penalty of $75,000.

The SEC order against Takeshi Uonaga, PAC's former CFO, alleged that Uonaga caused PAC to improperly record $82 million in revenue using a backdated contract and that he also made false representations to PAC's auditor regarding PAC's financial statements and internal controls. Uonaga neither admitted nor denied the finding of the SEC order against him. He agreed to pay a penalty of $50,000 and was suspended from practicing before the SEC as an accountant for a minimum period of five years.

11. PDVSA Procurement Prosecutions

On February 26, 2019, the DOJ unsealed an indictment that charged two Florida businessmen and Venezuelan nationals, Rafael Enrique Pinto Franceschi and Franz Herman Muller Huber, with foreign bribery, wire fraud, and money laundering for their alleged roles in a scheme to corruptly secure business advantages from Venezuela's state-owned energy company, Petroleos de Venezuela S.A. ("PDVSA"). These were only the latest individuals charged in a string of enforcement actions brought against alleged participants in the PDVSA procurement bribery scheme. In total, the DOJ has announced enforcement actions against 21 individuals in connection with its ongoing effort to prosecute the perpetrators of corruption at PDVSA; the majority of these individuals were U.S. based suppliers to PDVSA and have pleaded guilty to various charges related to the FCPA. Other charged individuals include former PDVSA employees or other Venezuelan government officials. Many of the enforcement

actions have led, among other things, to forfeiture orders of millions of dollars. Select highlights of the enforcement actions and the ongoing investigation are provided here.

a. Initial Enforcement against PDVSA Suppliers: Rincon, Shiera, and Associates

Roberto Enrique Rincon Fernandez (“Rincon”) and Abraham Jose Shiera Bastida (“Shiera”) were among the first set of enforcement actions, brought in December 2015. In approximately 2009, Rincon and Shiera initiated a coordinated effort to bribe PDVSA officials in exchange for new business and payment priority on outstanding invoices. Rincon and Shiera’s bribery scheme ran until approximately 2014. Shiera, based in Florida, and Rincon, based in Texas, owned multiple U.S.-headquartered energy companies that supplied equipment and services to PDVSA. In March 2016, Shiera pleaded guilty in the Southern District of Texas to one count of conspiracy violate the FCPA and to commit wire fraud, and one count of violating the FCPA. Three months later, Rincon pleaded guilty in the same jurisdiction to one count of conspiracy to violate the FCPA, one count of violating the FCPA, and one count of making a false statement on a tax return. The court imposed forfeiture orders against both individuals, requiring Shiera to surrender nearly $19 million. The forfeiture order against Rincon remains sealed. Sentencing for Rincon and Shiera is scheduled for February 1, 2020.

The DOJ also brought enforcement actions against associates and employees of Shiera and Rincon, including Moises Abraham Millan Escobar (“Millan”), Juan Jose Hernandez Comerma (“Hernandez”), and Fernando Ardila Rueda (“Ardila”). Millan, Shiera’s former employee, pleaded guilty in 2016 to one count of conspiracy to violate the FCPA for his role as an agent of both Shiera’s and Rincon’s companies in connection with the bribery scheme. Millan is sentenced to 3 years of probation and a fine of $15,000. In 2017, Hernandez, a former general manager and partial owner of one of Shiera’s companies, and Ardila, a former sales director and partial owner of several of Shiera’s companies, both pleaded guilty to one count each of violating and conspiracy to violate the FCPA in connection with their roles in the scheme. Hernandez and Ardila are scheduled to be sentenced on February 19, 2020. Another business owner, Charles Quintard Beech III (“Beech”), also pleaded guilty in 2017 to one count of conspiracy to violate the FCPA for his participation in a separate scheme to bribe PDVSA officials. Beech is scheduled to be sentenced on February 19, 2020.

b. Further Enforcement against PDVSA Suppliers: Castillo, Gonzalez & Pinto and Muller

On April 11, 2018, Juan Carlos Castillo Rincon (“Castillo”) was indicated on one count of conspiracy to violate the FCPA, three counts of violating and aiding and abetting violations of the FCPA, and one count of conspiracy to commit money laundering. Castillo, a naturalized U.S. citizen and resident of Texas, managed a Texas-based company that performed logistics services for PDVSA. According to the indictment, from 2011 until at least 2013, Castillo gained improper advantages from PDVSA Services, Inc. and PDVSA’s wholly owned U.S.-based purchasing subsidiary, by paying bribes to PDVSA officials. Some of the payments, which occurred in the U.S. or involved U.S. bank accounts, were specifically intended to induce the official to help Castillo’s company win contracts, provide Castillo with insider information, or request advantageous modifications of existing contracts between Castillo’s company and PDVSA. The indictment further alleges that Castillo attempted to conceal those payments by submitting fraudulent invoices for services never performed. Castillo pleaded guilty to a single count of conspiracy to violate the FCPA and is awaiting sentencing that is scheduled for February 20, 2020.

On May 29, 2019, Jose Manuel Gonzalez-Testino (“Gonzalez”) pleaded guilty to one count of conspiracy to violate the FCPA, one count of violating the FCPA, and one count of failing to report foreign bank accounts. Authorities arrested Gonzalez on July 31, 2018 at Miami International Airport. According to an affidavit in support of the criminal complaint, Gonzalez, a dual U.S.-Venezuelan citizen, controlled multiple energy companies based

in the U.S. and Panama that supplied products and services to PDVSA. The affidavit alleges that Gonzalez and others conspired to bribe PDVSA officials in exchange for receiving favorable treatment for Gonzalez's companies. Specifically, the government alleges that Gonzalez paid at least $629,000 to a former PDVSA official in exchange for new contracts, payment priority, and favorable contract terms such as payment in U.S. dollars instead of Venezuelan bolivars. The affidavit further states that two former PDSVA officials, including the one that Gonzalez allegedly bribed, have already pleaded guilty in connection with the PDVSA bribery scheme and are cooperating with authorities. Gonzalez is scheduled to be sentenced on November 19, 2019.

As noted in the introduction, on February 21, 2019, the DOJ charged Rafael Enrique Pinto Franceschi ("Pinto") and Franz Herman Muller Huber ("Muller"). According to the indictment, Muller was the president of a Miami-based supplier of heavy equipment to PDVSA; Pinto was a sales representative with the same company. Pinto and Muller are each charged with one count of conspiracy to violate the FCPA, one count of conspiracy to commit wire fraud, two counts of wire fraud, and one count of conspiracy to launder money. The indictment states that from 2009 to 2013, Pinto and Muller conspired with others to bribe three PDVSA officials in exchange for providing assistance in connection with their company's PDVSA business. The PDVSA officials allegedly assisted Pinto and Muller's company in obtaining additional PDVSA contracts, inside information, and payment on past due invoices. In total, Pinto and Mueller are alleged to have received over $985,000 and $258,000, respectively, in kickback payments as part of this scheme (forming the basis for the wire fraud charges.)

c. Enforcements Against Former PDVSA / Government Officials, including De Leon, Cesar Rincon, Villalobos, Reiter, Isturiz & Camacho & Guedez

The DOJ also charged former PDVSA officials involved in the scheme initiated by Rincon and Shiera. December 2015 saw the first string of guilty pleas (to conspiracy to commit money laundering for accepting and attempting to conceal bribes) from PDVSA officials including Jose Luis Ramos Castillo, Christian Javier Maldonado Barillas, Alfonzo Eliezer Gravina Munoz. Similarly, in October 2016, Karina Del Carmen Nunez-Arias, a former purchasing analyst for Bariven S.A. ("Bariven"), PDVSA's equipment procurement subsidiary, pleaded guilty to one count of conspiracy to violate the FCPA and to commit money laundering. These cases have resulted in money judgments/forfeitures as well as probation/prison sentences, (the latter, with the exception of Alfonzo Eliezer Gravina Munoz, who still awaits sentencing in November 2019).

On February 12, 2018, the DOJ announced charges against five further former Venezuelan government officials for their alleged roles in the bribery scheme that also involved Rincon and Shiera. Two of the individuals (Luis Carlos de Leon-Perez and Nervis Gerardo Villalobos Cardenas) acted as conduits for the bribe payments initiated by Rincon, Shiera and others. The other three (Cesar David Rincon-Godoy ("Cesar Rincon"), Rafael Ernesto Reiter-Munoz ("Reiter"), and Alejandro Isturiz-Chiesa ("Isturiz")) were PDVSA employees during the relevant period and recipients of the bribe payments.

The 18-count indictment, dated August 23, 2017, charged De Leon and Villalobos with conspiracy to violate the FCPA, conspiracy to commit money laundering, and committing money laundering for their role in directing and disguising bribe payments from Rincon, Shiera, and others to PDVSA officials. The indictment alleged that between 2011 and 2013, Rincon and Shiera sent more than $27 million in bribe payments to a Swiss bank account controlled by De Leon and Villalobos. De Leon and Villalobos then transferred the funds to other Swiss accounts to pay bribes to PDVSA officials, including Cesar Rincon, Reiter, and Isturiz. De Leon and Villalobos, who had previously held positions as foreign officials in Venezuela, were private citizens at the time of the alleged conduct. In October 2017, De Leon, Villalobos, Cesar Rincon, and Reiter were arrested in Spain at the request of U.S. authorities. De Leon and Cesar Rincon were subsequently extradited to the U.S. Villalobos and Reiter remain in Spanish custody pending extradition. Isturiz's whereabouts are unknown.

On July 16, 2018, De Leon, a dual citizen of the U.S. and Venezuela, pleaded guilty to one count of conspiracy to violate the FCPA and one count of conspiracy to commit money laundering. De Leon admitted that he conspired with Villalobos, Cesar Rincon, Isturiz, and others to solicit bribes from Rincon and Shiera for PDSVA officials. In exchange, Rincon and Shiera obtained business advantages and received payment priority on outstanding invoices. De Leon further admitted that he conspired to launder and conceal the funds through various financial transactions, including wire transfers to accounts in Switzerland held in the name of individuals or entities other than De Leon and his co-conspirators.

On April 19, 2018, Cesar Rincon, former general manager of Bariven, pleaded guilty to one count of conspiracy to commit money laundering. Cesar Rincon admitted to accepting and attempting to conceal bribes from Rincon and Shiera while he was a PDVSA official in exchange for offering payment priority and new contracts to Rincon's and Shiera's companies. The court ordered Cesar Rincon to forfeit approximately $7 million, equal to the amount of bribe payments he admitted to accepting. Cesar Rincon is awaiting sentencing.

Finally, Jose Orlando Camacho and Ivan Alexis Guedez, two of the three officials accused of having been bribed by Miami-based PDVSA suppliers Pinto and Muller, were charged with conspiracy to commit money laundering and have pleaded guilty. Camacho and Guedez are awaiting sentencing, which is scheduled for February 20, 2020.

12. Petrobras

Key Facts:

Agencies: DOJ; SEC; Brazilian MPF
Countries Involved: Brazil
Amount of Total Financial Settlement: $853.2 million
Means of Corruption: Sham business transactions, inflated contracts

On September 27, 2018, Petrobras reached simultaneous agreements with authorities in the United States and Brazil in relation to a series of massive bribery and bid-rigging schemes overseen by Petrobras executives and others over the course of nearly a decade. In the U.S., Petrobras entered into a Non-Prosecution Agreement (the "NPA") with the DOJ and a settlement with the SEC, which resulted in a cease and desist order ("Order"). In Brazil, Petrobras entered an agreement to reach a settlement with Brazil's Federal Prosecution Service, the Ministério Público Federal ("MPF"). At all relevant times, Petrobras's common and preferred stock was registered with the SEC pursuant to Section 12(b) of the Exchange Act and traded on, inter alia, the New York Stock Exchange as American Depositary Shares ("ADSs"), making Petrobras a U.S. issuer for the purposes of FCPA jurisdiction.

According to the charging documents, from at least 2003 to 2012, senior Petrobras executives colluded with Petrobras's largest contractors and suppliers to intentionally inflate the cost of Petrobras's ongoing infrastructure projects by billions of dollars. The Petrobras executives took kickbacks in the range of 1-3% from these inflated contracts. Executives then passed along a portion of this money to the Brazilian politicians who had helped install the executives in their roles at Petrobras. For example, in 2005, Petrobras announced its intention to complete the construction of the Abreu e Lima Refinery ("RNEST") in Brazil. Certain Petrobras executives worked together to ensure that certain contractors were invited to bid for the various contracts involved in the RNEST construction. One executive shared with the cartel of bidders the final list of contractors that would be invited to facilitate coordination among the bidders to rig the process. According to the SEC, in exchange for the information and the structuring, the winning contractor paid hundreds of millions of dollars to the Petrobras officials and certain politicians and political parties.

Per the SEC Order and NPA, Petrobras did not have in place a system of internal controls sufficient to provide reasonable assurances that SEC and other filings were accurate and, in fact, the SEC noted a number of material misstatements and omissions in Petrobras's financial statements and Forms 20-F from 2009 – 2013. For example, Petrobras included the kickbacks from the corruption scheme in the carrying amount of the company's property, plant, and equipment ("PP&E") in the company's 20-F forms filed starting in May 2010 and through 2014. In its Form 6-K for the quarter ending September 30, 2014, Petrobras ultimately wrote off nearly $2.6 billion of capitalized costs, representing the estimated overpayment amounts attributable to the kickbacks included in the inflated PP&E. The SEC noted a number of other misstatements, including with regard to the qualifications of its executives who, the SEC noted, were not chosen by virtue of their knowledge or specialization, but rather due to their roles in a corrupt patronage system. Certain executives were found to have knowingly and willfully failed to implement a sufficient system of internal controls to facilitate the payment of illegal bribes.

The SEC Order and NPA detail not just a single corrupt scheme, but a widespread practice of corruption among senior Petrobras executives. In one illustrative example included in the SEC Order, a Petrobras executive directed the purchase of a Texas oil refinery from a Belgium company in 2006, despite the fact that the executive was aware that the refinery had deteriorated and that its oil did not meet Petrobras's needs. In return for directing the purchase, the executive received a $2.5 million bribe.

Petrobras consented to the entry of the SEC Order, which asserted claims against Petrobras for violations of the books and records and internal controls provisions of the FCPA as well as violations of Sections 17(a)(2) and 17(a)(3) of the Securities Act and Section 13(a) the Exchange Act. In accepting Petrobras's offer of settlement, the SEC noted Petrobras's "significant" cooperation, including the fact that Petrobras has served as "Assistant to the Prosecution" in 51 proceedings in Brazil. The SEC also noted various critical remedial measures taken by Petrobras, including enhancing the compliance function, creating a Division of Governance and Compliance, enhancing controls around procurement and due diligence of contractors, and replacing the entire Board of Directors and Executive Board.

Under the terms of the NPA, Petrobras accepted its responsibility under U.S. law for the books and records and internal controls violations of its officers, directors, employees, and agents. Petrobras also committed to, among other actions, continue to improve its compliance program and trainings, conduct periodic risk-based reviews, and report at least annually to the DOJ during the three-year term of the NPA.

Petrobras agreed to pay a total penalty of $853.2 million. The total penalty reflected a 25% reduction off the bottom of the U.S. Sentencing Guidelines fine range. The reduction was granted to Petrobras on the basis of its cooperation with U.S. and Brazilian authorities and its remediation efforts, including its completion of a "thorough and timely" internal investigation, replacement of its Board of Directors and Executive Board, and introduction of an enhanced compliance program. Under the terms of the various agreements, the total penalty was divided, with Petrobras agreeing to pay $85.32 million (10%) each to the DOJ and SEC and $682.56 million (80% of the total penalty) to Brazilian authorities. The Brazilian payment does not include an attribution of liability and will be allocated to social and educational programs to promote integrity and transparency in the public sector in Brazil.

In addition to the $853 million penalty, Petrobras agreed to pay a total of $933 million in disgorgement and prejudgment interest to the SEC. Per the SEC order, any payments made by Petrobras to the class action settlement fund created in the matter of *In re Petrobras Securities Litigation*, No. 14-cv-9662 (S.D.N.Y.) were to be credited against the required disgorgement and prejudgment interest payments. The class action settlement had been granted final approval in June 2018, with Petrobras agreeing to pay $2.95 billion to settle the lawsuit. The judge awarded a total of $186.5 million in attorneys' fees in the case. The class action settlement did not include an admission of guilt. In a securities filing released alongside the SEC and DOJ agreements, Petrobras

noted that the SEC would credit payments Petrobras had already made in relation to the class action, and confirmed that Petrobras would not make any additional payments to the SEC, beyond the $85.32 million penalty.

13. Polycom

Key Facts:

Agencies: SEC
Countries Involved: China
Amount of Total Financial Settlement: $36 million
Means of Corruption: Distributors

On December 26, 2018, Polycom, Inc. ("Polycom") agreed with the SEC to resolve charges that Polycom violated the books and records and internal accounting controls provisions of the FCPA in connection with misconduct in China. To resolve the matter with the SEC, Polycom agreed to an administrative cease and desist order, under which Polycom neither admitted nor denied the allegations, but agreed to pay a total of approximately $16 million in disgorgement, interest and a civil penalty. The same day, the DOJ and Polycom entered into a letter agreement under which the DOJ declined to prosecute Polycom for the same misconduct and Polycom agreed to pay an additional $20 million in disgorgement.

Headquartered in San Jose, California, Polycom is a telecommunications company that sells voice and video communications equipment throughout the world. At the time of the misconduct, Polycom Communications Solutions (Beijing) Co., Ltd. ("Polycom China") was a wholly owned subsidiary of Polycom that sold Polycom products in China through a network of distributors and resellers. During the relevant period, Polycom's stock was publically traded on the Nasdaq Global Select Market.

According to the SEC, from 2006 through at least July 2014, Polycom China used its network of distributors to make improper payments to Chinese government officials in order to obtain business with state-owned entities. Polycom China personnel allegedly sold products to certain distributors at a discount, with the understanding that the discounts would be used to fund the improper payments. The SEC alleged that in order to conceal this scheme, Polycom China recorded sales activities in a local and unapproved database that was separate from Polycom's centralized customer relations management database. Polycom personnel outside of China were unaware of this parallel system. Polycom China personnel allegedly recorded the real justifications for the discounts in this off-line system for approval by Polycom China management. The SEC indicated that Polycom China's senior managers recorded the discounts in Polycom's legitimate database, but indicated that the discounts were being passed on to the customers as a legitimate means of winning business in China. Polycom China's senior managers also allegedly directed Polycom China's sales personnel to use non-Polycom email addresses when discussing deals with the Chinese distributors.

Discounts above a certain threshold required Polycom China to obtain approval from Polycom managers in Singapore. According to the SEC, Polycom China senior managers routinely cited legitimate reasons for the need for the discounts, such as budget constraints of the customers or tight competition.

According to the SEC, Polycom's internal controls were inadequate and failed to detect and prevent the fraudulent justifications for the discounts as well as the resulting improper payments. Polycom's compliance program also fell short in a number of areas, including the failure to translate anti-corruption policies into Chinese, the failure to ensure that all relevant personnel completed compliance training, and the failure to address red flags identified in due diligence on certain distributors.

The SEC indicated that from 2012 to 2014, the improper payments generated over $10 million in profits. As part of its settlement with the SEC, Polycom was required to disgorge this full amount plus an additional $1.8 million in interest. Polycom was also required to pay a $3.8 million civil penalty to the SEC.

In calculating this penalty and agreeing to the settlement, the SEC took into account several mitigating factors, including that Polycom had hired outside counsel to conduct an independent internal investigation, self-disclosed the misconduct, cooperated with the SEC's investigation, terminated the employment of a number of personnel involved in the misconduct, terminated the company's relationship with certain distributors, improved its anticorruption and other training, hired additional personnel to enhance compliance oversight, and otherwise improved its compliance program and internal controls.

Through a letter agreement, the DOJ invoked the Corporate Enforcement Program and declined to prosecute Polycom despite finding that the conduct violated the FCPA. The DOJ did require, however, that Polycom disgorge an additional $10.15 million of profits to the Treasury Department, and a further $10.15 million to the U.S. Postal Inspection Service Consumer Fraud Fund. The DOJ explained that it reached its declination decision based on a number of factors, including that Polycom had self-disclosed the misconduct, conducted a thorough investigation, cooperated with the DOJ's investigation, and undertaken the remedial measures discussed above.

14. Eberhard Reichert—Siemens

Key Facts:

Agencies: DOJ
Countries Involved: Argentina
Means of Corruption: Third-party intermediaries

On March 15, 2018, seven years after he was first indicted, Eberhard Reichert, the former Executive Director for Foreign Data Processing at Siemens Business Services GmbH & Co. OGH ("SBS"), a subsidiary of Siemens Aktiengesellschaft ("Siemens"), pleaded guilty to one count of conspiracy to violate the FCPA's anti-bribery provisions, accounting provisions, and wire fraud. Reichert, along with seven co-conspirators, were first charged in 2011 in connection with a decades-long scheme to bribe Argentinian officials in connection with a national identity card project valued at approximately $1 billion.

As discussed in-depth in the analysis of Siemens' 2008 settlement (*see* Hughes Hubbard FCPA & Anti-Bribery Compendium, "Siemens"), Siemens and its subsidiary in Argentina paid over $100 million to current and former Argentine government officials between 1996 and 2009 as part of its campaign to win and maintain the identity card project. Many of these payments were made through a consulting group that funneled money to high-level Argentine officials who could influence the project. Other payments were made to entities controlled by members of the Argentine government and to other entities that acted as conduits for bribes.

In December 2011, the DOJ indicated eight former Siemens executives and agents, alleging that they participated in the bribery scheme in Argentina. According to the indictment, Reichert worked for Siemens from 1964 until about 2001. Among other things, Reichert was involved in the scheme to pay millions of dollars to entities that purportedly provided services for Siemens, but which merely served as conduits for bribe payments to various Argentinian officials and politicians. Reichert participated in meetings in which these illicit payments were planned, and also signed contracts with the conduit entities. Reichert was also involved in a transaction in which a fake foreign currency hedging transaction was used to conceal improper payments to Argentinian officials.

Reichert was arrested in Croatia in September 2017 and voluntarily agreed to be extradited to the United States in December 2017. In March 2018, he pleaded guilty to one count of conspiracy to violate the FCPA and commit wire fraud, and is currently awaiting sentencing. Reichert is only the second of the eight defendants to face U.S. charges. In 2015, Andres Truppel, the former CFO for Siemens Argentina, pleaded guilty to the same charge of conspiracy to violate the FCPA and commit wire fraud. Truppel is also still awaiting sentencing. The six remaining defendants are all still at large.

15. Sanofi

Key Facts:

Agencies: SEC
Countries Involved: Kazakhstan, Lebanon, UAE
Amount of Total Financial Settlement: $25.3 million
Means of Corruption: Distributors, excessive samples, travel and entertainment

On September 4, 2018, the SEC accepted an offer of settlement from the French pharmaceutical giant Sanofi, resolving claims that Sanofi violated the FCPA's internal accounting controls and recordkeeping provisions. The SEC alleged that Sanofi subsidiaries organized in Kazakhstan, Lebanon, and the United Arab Emirates (UAE) made and kept false records of improper payments to healthcare professionals in exchange for the distribution of Sanofi products. The accounts and records of these subsidiaries were rolled up into Sanofi's books and records. Sanofi agreed to pay disgorgement in the amount of $17.6 million, prejudgment interest of $2.7 million, and a civil penalty of $5 million.

The SEC alleged that from 2007 to 2011, employees of Sanofi's Kazakh subsidiary engaged in a scheme to bribe Kazakh officials, with the assistance of local distributors, in order to influence the award of public tenders to Sanofi. The multistage process involved conspiring with distributors to inflate the sales price of products to fulfill public tenders and using the difference between the public sales price and the price Sanofi charged the distributors (typically a 20-30% difference) to create a slush fund from which bribes could be paid. Once Sanofi and the distributor agreed on an amount to be paid as a bribe, the distributor would return that amount to Sanofi employees (out of the created slush fund) to deliver to the Kazakh officials. These payments were referred to in internal records as "marzipans." According to the SEC, Sanofi earned approximately $11.5 million in profit using this scheme.

Employees of Sanofi's Lebanese subsidiary allegedly engaged in various schemes between 2011 and 2013 to increase Sanofi product sales through prescriptions. As one example, the SEC described a request by a healthcare professional at a large hospital in Jordan for several samples of an expensive cancer drug. This individual was a member of the hospital's tender committee. Although Sanofi's corporate policy required a medical justification for the cancer drug's distribution, the SEC alleged that no such justification was recorded in reviewing or approving the distribution of these drugs to the healthcare professional. Sanofi's subsidiary provided the healthcare professional 24 vials of the drug as "samples," equal to nearly 20% of the hospital's purchases of the drug. The SEC alleged that Sanofi also paid this individual over $160,000 in undocumented consulting, speaking, and clinical trial fees. Through this and other similar schemes in the region, Sanofi alleged derived profits of approximately $4.2 million.

From 2012 to 2015, sales managers and medical representatives in Sanofi's Gulf operations allegedly perpetuated a scheme to submit false travel and entertainment expenses and use the unwarranted reimbursement in order to corruptly compensate local healthcare professionals for increasing prescriptions of Sanofi products. As part of the scheme, medical representatives were instructed by local sales managers to submit false reports and doctored receipts for round table meetings with doctors that never occurred. The sales managers approved the reimbursement of costs related to these fabricated events and the proceeds were used to create a slush fund from which to make corrupt payments to health care professionals to increase prescriptions of Sanofi products. According to the SEC, Sanofi earned profits of approximately $1.75 million through this scheme.

All told, Sanofi's alleged violations resulted in profits of over $17 million. The SEC recognized Sanofi's pre-settlement remedial actions, which included providing regular briefings of its internal investigation to SEC staff, updating its internal controls and procedures governing interactions with local healthcare professionals, posting compliance personnel in high-risk local markets, terminating or disciplining over 160 employees, and accepting the resignation of 14 other employees.

In addition to its agreement to pay approximately $25 million to resolve these claims, Sanofi agreed to make three reports to the SEC over a two-year time period detailing its remedial efforts, submit any external audit reports generated during the two-year period, and cooperate with the SEC's investigations and other proceedings arising out of the allegations set forth in the settlement.

16. Société Générale and Legg Mason

Key Facts:

Agencies: DOJ; SEC; PNF (France)
Countries Involved: Libya
Amount of Total Financial Settlement: $585 million (SGA); $64.2 million (Legg Mason)
Means of Corruption: Third-party agent

On June 4, 2018, Société Générale S.A. ("Société Générale"), a global financial institution headquartered in Paris, France, and its wholly-owned subsidiary, SGA Société Générale Acceptance N.V. ("SGA"), agreed to pay a total of $585 million to U.S. and French authorities in order to resolve a coordinated investigation into a multi-year scheme to bribe Libyan foreign officials. With the DOJ, Société Générale entered into a three-year deferred prosecution agreement ("DPA") and agreed to pay a total criminal penalty of $585 million to resolve one count of conspiracy to violate the anti-bribery provisions of the FCPA. The DPA also settled a second count relating to the Société Générale's attempted manipulation of and false reporting in connection with London Interbank Offered Rate (LIBOR) for the U.S. Dollar and Yen.

SGA pleaded guilty in the Eastern District of New York ("EDNY") to one count of conspiracy to violate the anti-bribery provisions of the FCPA and was fined $500,000 (credited against Société Générale's total criminal penalty).

Société Générale also reached a settlement with Parquet National Financier (PNF) in Paris related to the same conduct, agreeing to pay approximately $293 million. The DOJ credited the amount agreed to be paid by Société Générale to the PNF against the total criminal penalty agreed in the DPA.

On the same day, Société Générale's co-conspirator, Maryland-based investment management firm, Legg Mason Inc. ("Legg Mason") and its subsidiary, Permal Group Ltd. (Permal), agreed to pay $64.2 million in criminal penalties and enter into a non-prosecution agreement ("NPA") to settle charges with the DOJ related to the same scheme. Three months later, on August 27, 2018, the SEC issued a cease and desist order against Legg Mason for books and records and internal controls violations of the FCPA for the same underlying conduct. Under the SEC order, Legg Mason agreed to $28 million in disgorgement and $7 million in prejudgment interest.

a. The Bribery Scheme

After the easing of economic sanctions against Libya in 2004, the Libyan sovereign wealth fund (Libyan Investment Authority ("LIA")) and other Libyan state institutions sought to invest substantial funds with international financial institutions. To secure investments, Permal and Société Générale conspired to funnel bribes to multiple Libyan officials through a Libyan-Italian agent ("Agent"). The Agent was "the right arm" and the "enforcer" of a close relative (and a bribe payment recipient) of then-Libyan dictator Muammar Gaddafi.

In total, between 2005 and 2009, Société Générale and Legg Mason paid approximately $91 million in bribes to the Agent for "introduction" services, passed through the Agent's company incorporated in Panama. Portions of these payments were then passed on to high-level Libyan officials to secure 13 investments and one restructuring, valued at $3.66 billion. Société Générale earned profits of approximately $523 million from these deals. Seven of the 13 investment notes Société Générale sold to the Libyan state institutions (valued at $950

million) were linked in whole, or in part, to Permal. In connection with these seven transactions, Permal earned net revenues of approximately $31.6 million.

By at least 2006, two Permal employees and several Société Générale employees knew that the Agent was paying money and providing other improper benefits to Libyan government officials in order to secure lucrative investments and exclude competitors for the benefit of Permal and Société Générale. Despite that knowledge, these employees agreed to continue to use the Agent who, through the use of bribes or coercion, exerted influence over (or “cooked”) relevant Libyan officials.

Permal and Société Générale also deployed measures to conceal the bribery scheme. In addition to using coded terms such as “cooked,” in 2006, Permal and Société Générale conspired to hide the Agent’s existence by replacing the Agent’s name in relevant documents with Permal’s name, and then using Permal to pass the payments to the Agent. Later, Permal and Société Générale, with the help of the Agent, conspired to persuade the LIA to amend its agent disclosure requirement to be “forward looking only,” so that the past relationship with the Agent could be concealed.

Around November 2009, compliance personnel at Société Générale Corporate and Investment Bank (“SG CIB”), a division of Société Générale that offered investment banking services, indicated to their senior managers that the commissions paid to the Agent appeared unjustifiable in relation to the service rendered, based on the amounts paid and the percentage to the investment deals. The compliance personnel also raised concerns that the Agent was paid through a Panamanian company, incorporated in a country that is on the OECD’s blacklist. Despite these alarms, Société Générale continued to seek to engage the Agent in a variety of capacities, including as a joint venture partner.

In mid-2010, LIA’s new management made inquiries to Société Générale employees about the role of the Panamanian entity on various prior deals and the entity’s owner. Following these inquiries, Société Générale’s employees provided false and misleading information to LIA, including falsely stating that the remuneration paid to the Panamanian company did not affect the profitability of LIA’s investments and that the company complied with all of Société Générale’s internal procedures. Société Générale also failed to respond to certain inquiries and minimized disclosures in term sheets by using small font and non-standard typefaces.

b. Terms of the Resolutions

Société Générale’s total criminal penalty reflects a 20% discount off of the low end of the calculated U.S. Sentencing Guidelines fine range. According to the DPA, the discount was attributed to Société Générale’s efforts to conduct a thorough and robust internal investigation, collect and produce voluminous evidence located in other countries, and provide frequent and regular updates to authorities as to the status of and facts learned. Because the DOJ had developed significant independent evidence of misconduct without Société Générale’s assistance, Société Générale did not receive the full 25% reduction for which it was eligible. The DOJ agreed that an independent compliance monitor was unnecessary because of Société Générale’s remediation and the advanced state of its compliance program.

In addition to the DPA with the DOJ, Société Générale settled a civil dispute with the LIA and made a payment of approximately $1.1 billion to the LIA relating to the allegations of corruption.

Legg Mason’s criminal penalty represented a 25% discount off of the low end of the calculated U.S. Sentencing Guidelines range, attributed to Legg Mason’s substantial cooperation and remediation. In reaching the NPA, the DOJ acknowledged several mitigating factors, including: (i) the misconduct only involved two mid-to-lower level employees of Permal, a Legg Mason subsidiary; (ii) relevant employees had been disassociated with Permal for

more than four years at the time of the NPA; (iii) the misconduct was not pervasive throughout the company; (iv) it was Société Générale, the co-conspirator, not Legg Mason itself, that maintained the relationship with the Agent and was responsible for originating and leading the scheme; (v) the profits earned by Legg Mason from the misconduct were less than one-tenth of the profits earned by Société Générale; and (vi) Legg Mason has no history of similar misconduct.

In declining to impose a civil penalty, the SEC also recognized Legg Mason's significant cooperation in collecting information that might not have been otherwise available to the SEC. This cooperation included summarizing the findings of its internal investigation, making employees available to the SEC (including arranging for foreign employees' travel to the United States for interviews), and providing timely factual summaries of witness interviews and other information developed in the course of its internal investigation. The SEC also considered Legg Mason's remedial action, including disciplining the employees involved in the violation, expanding the compliance function, and enhancing its internal accounting controls to prevent and detect the type of similar misconduct in the future.

17. Stryker

Key Facts:

Agencies: SEC
Countries Involved: China, India, Kuwait
Amount of Total Financial Settlement: $7.8 million
Means of Corruption: Third-party dealers, distributors

On September 28, 2018, Stryker Corporation agreed to settle charges with the SEC that it had violated the FCPA's books and records and internal accounting controls provisions through its operations in China, India, and Kuwait. As part of the resolution, without admitting or denying the allegations, Stryker agreed to pay a $7.8 million civil penalty and to appoint an independent compliance consultant for a period of 18 months to review and evaluate Stryker's ethics and compliance function, internal controls, record-keeping, and anti-corruption policies and procedures, especially regarding third parties such as dealers, agents, distributors, and sub-distributors. The independent compliance consultant will issue a written report within six months of being retained, after which Stryker will have 90 days to implement any recommendations. After 180 days, the Compliance Consultant will perform a follow-up review.

Stryker had previously paid $13.2 million to settle charges with the SEC in October 2013 that it had violated the FCPA's books and records and internal accounting controls provisions with regard to improper payments made to doctors and officials at government-run hospitals in Argentina, Greece, Poland, and Romania. The SEC alleged that Stryker had falsely recorded these expenses as charitable donations, consultant fees, travel expenses, and commission payments.

Stryker is a Michigan-based producer of medical technologies including implants, surgical equipment, medical devices, and emergency medical equipment. At all relevant times its shares were registered with the SEC under section 12(b) of the Exchange Act and were traded on the New York Stock Exchange, making it an "issuer" under the FCPA.

a. Misconduct in China, India, and Kuwait

In India, Stryker's wholly-owned subsidiary Stryker India generated 85% of its sales revenue through sales to third-party dealers. Stryker's global compliance and accounting policies and procedures applied to each dealer, including a prohibition on improper payments to government or non-government officials, employees, or entities and a requirement for each dealer to maintain complete and accurate records regarding their distribution of

Stryker products. According to the SEC, in 2012, Stryker India received allegations of misconduct by its dealers and investigated three, finding inadequate record-keeping and internal accounting controls at all three. One dealer was terminated and certain corrective actions were implemented regarding the remaining two dealers investigated. However, despite numerous red flags and complaints, the SEC alleges that Stryker India failed to perform an audit of the rest of its third-party dealers until 2015. According to the SEC, the 2015 audit revealed that Stryker India's inadequate controls had allowed its dealers to submit inflated invoices to hospitals at their request so that the hospitals could pass along the falsely inflated charges to patients and their insurance carriers. The SEC further alleges that Stryker India failed to maintain accurate books and records and repeatedly authorized payments to third parties without documentation to establish a legitimate business purpose. Upon examination of a sample of Stryker India's highest-risk transactions, the SEC found that over 27% had no accompanying documentation whatsoever.

In China, Stryker's wholly-owned subsidiary, Stryker China, sold products through a state-owned "hub"-distributor that, in turn, re-sold products through a network of sub-distributors. According to the SEC, between 2015 and 2017 at least 21 sub-distributors sold Stryker's products in China without going through any type of review, approval, or training by Stryker China. The SEC alleged that, in some cases, third, fourth, and fifth tier sub-distributors were even engaged to sell Stryker's products, all without approval or training and in violation of Stryker's accounting controls policies. Furthermore, the SEC alleged that in certain cases Stryker China employees worked directly with the unauthorized sub-distributors and, in other cases, purposefully concealed the involvement of the sub-distributors. According to the SEC, Stryker's deficient internal accounting controls failed to detect or prevent the use of unauthorized and untrained sub-distributors, increasing the risk that Stryker funds could have been used to pay bribes or fund other types of misconduct.

In Kuwait, employees of Stryker's Netherlands-based wholly-owned subsidiary oversaw sales of Stryker products to the Kuwait Ministry of Health through one primary distributor. From 2015 to 2017, Stryker allegedly held a number of events for Kuwaiti healthcare providers where Stryker paid for meals, accommodations, and local travel directly. However, according to the SEC, Stryker's Kuwaiti distributor paid $32,000 in additional "per diems" related to these events that were not detected by Stryker's internal accounting controls. According to the SEC, when Stryker tried to exercise its audit rights, the distributor refused. As a result, the SEC alleged that Stryker's internal accounting controls had failed to test or otherwise assess whether the distributor was complying with Stryker's anti-corruption policies.

b. Remediation

The SEC considered Stryker's cooperation and remedial efforts in reaching the settlement. In terms of cooperation, the SEC pointed to the facts that Stryker hired counsel to conduct an internal investigation into its operations in India, China, and Kuwait and shared its findings with the SEC on an ongoing, voluntary basis in cooperation with the SEC's own investigation. Stryker also updated its policies and procedures in India, introduced additional controls around its monitoring of dealership and distributorship relationships, created new third-party due diligence controls, increased training for all Stryker India employees, created a centralized system for documentation to increase transparency in India, conducted compliance audits of marketing events and reimbursements in India, and audited its dealers' and distributors' business practices in India. Stryker also appointed new leadership for Stryker India, terminated senior employees at Stryker India, terminated its distributor in Kuwait, and strengthened its compliance program with special attention to due diligence and documentation related to consultants and distributors.

18. Transport Logistics International and Mark Lambert

Key Facts:

Agencies: DOJ
Countries Involved: Russia
Amount of Total Financial Settlement: $2 million
Means of Corruption: False invoices, sham agreements

On January 1, 2018, the DOJ charged Transport Logistics International, Inc. ("TLI") with conspiracy to violate the anti-bribery provisions of the FCPA in order to obtain and retain uranium transportation contracts. Two months later, the company entered into a three-year Deferred Prosecution Agreement related to the charges. Under the DPA, TLI agreed to pay a $2 million penalty. TLI also agreed to institute an enhanced compliance program and conduct a review of its internal accounting controls. Given its size and risk profile, TLI was not required to retain an independent compliance monitor.

On January 12, 2018, the DOJ also unsealed an 11-count indictment against former TLI owner and executive Mark Lambert. Lambert faces one count of conspiracy to violate the FCPA and to commit wire fraud, seven counts of violating the FCPA, two counts of wire fraud, and one count of money laundering. Lambert is only the latest individual prosecuted in connection with the scheme; the DOJ secured guilty pleas from three other individuals in 2015 for related conduct.

a. TLI

TLI is a Maryland-based transportation company that provides shipping services for nuclear materials both within the United States and abroad. The charges against TLI arose from its role in the so-called "Megatons to Megawatts" project, an agreement between the U.S. and Russia for the disposal of enriched uranium from disassembled Russian warheads by downgrading and selling it to U.S. nuclear energy providers. From 1995 until 2013, the program saw the conversion of 475 metric tons of high-grade uranium—the equivalent of 19,000 warheads—into low-grade uranium, which was then sold in the U.S. JSC Techsnabexport ("TENEX"), a subsidiary of Russia's State Atomic Energy Corporation ("ROSATOM"), was responsible for the sale and transportation of this vast quantity of material to the U.S. TENEX selected TLI as one of its transportation providers.

According to admissions by TLI, from 2004 to 2014, TLI and certain individuals conspired to pay approximately $1.7 million in bribes to Russian national Vadim Mikerin (at the time a Director of TENEX) to secure improper advantages in gaining and retaining business with TENEX. The co-conspirators discussed the bribes in coded language and created false invoices to disguise TLI's illicit payments. In one example, then-TLI owner and executive Daren Condrey instructed a TLI employee to create an invoice for $8,157 to "get commissions off the books." TLI then paid that amount to a bank in Cyprus based on the fraudulent invoice. The following day, another co-conspirator wrote Mikerin to confirm the payment, stating that "Cake was delivered yesterday as planned." Mikerin used similar language to request bribes, asking, for example, that a certain co-conspirator "please confirm [his] ability to support TLI's Cake Cooking on a regular basis once per [quarter] at 5% net volume." In exchange for these kickbacks, Mikerin ensured that TENEX would continue to award contracts to TLI.

In determining the appropriate fine for TLI's misconduct, the DOJ noted TLI's failure to voluntarily and timely disclose its conduct and thus declined to provide any voluntary disclosure credit. The DOJ did, however, provide TLI with full credit for its substantial cooperation in the investigation. Specifically, TLI earned credit for reviewing emails and financial statements, voluntarily producing pertinent documents, and providing interviews with relevant witnesses, including one Russian witness who was otherwise inaccessible to prosecutors. TLI also provided information about the other individuals involved in the misconduct and engaged in remedial measures up to and

including termination of all individuals who participated in the scheme. The DOJ granted TLI a 25% reduction off the lower end of the sentencing range for its cooperation and remediation and determined the appropriate penalty was $21,375,000. The 25% reduction is the maximum allowable for a company that does not voluntarily disclose misconduct per the DOJ's FCPA Corporate Enforcement Policy.

However, TLI represented that a penalty greater than $2 million would substantially jeopardize the company's continued viability. Based on that representation, and after conducting an independent ability-to-pay analysis, the DOJ determined that that a penalty of $2 million was appropriate. The DOJ also credited approximately $220,000 in seized funds against the penalty.

b. Mark Lambert and Other Individuals

The DOJ brought charges against Mark Lambert, former owner and executive of TLI, alongside Condrey, for alleged acts that closely track the charges for which Condrey and TLI pleaded guilty. The DOJ alleges that Lambert and Condrey learned of the conspiracy in 2009 from an undisclosed TLI executive, and soon agreed to take part in it. In addition to the schemes described above—the use of code words to conceal the payment of bribes, and the fraudulent creation of invoices to effect those payments—the DOJ alleges that Lambert personally authorized many of the wire transfers TLI made to shell corporations for the ultimate benefit of Mikerin. Lambert's trial is scheduled to begin in October 2019.

Several other individuals have already pleaded guilty to FCPA violations and other offenses in connection to the same bribery scheme. On June 16, 2015, the DOJ charged Condrey with conspiracy to violate the FCPA and conspiracy to commit wire fraud, and he pleaded guilty the following day. He is awaiting sentencing as of the time of this writing.

On August 31, 2015, Mikerin pleaded guilty to one count of conspiracy to commit money laundering. On December 15, 2015, Mikerin was sentenced to 48 months in prison. He was also ordered to forfeit $2,126,622.36—the amount transferred to offshore bank accounts in the course of the scheme.

On June 15, 2015, Boris Rubizhevsky pleaded guilty to conspiracy to commit money laundering for his participation in the scheme, which involved providing sham consulting services as a means to disguise payments to TENEX. He was sentenced to one year and one day in prison, followed by three years of supervised release, and was also ordered to forfeit $26,500.

19. United Technologies

Key Facts:

Agencies: SEC
Countries Involved: Azerbaijan, China, Kuwait, Russia, Pakistan, South Korea, Thailand, Indonesia
Amount of Total Financial Settlement: $13.9 million
Means of Corruption: Subcontractors, distributors, agents, sponsorships, travel and entertainment

On September 12, 2018, United Technologies Corporation ("UTC") agreed to pay $13.9 million to resolve allegations that it violated the anti-bribery, books and records, and internal controls provisions of the FCPA through payments by subsidiaries in UTC's elevator and aircraft engine businesses. Without admitting or denying the allegations, UTC consented to the SEC's cease and desist order ("Order") alleging that UTC subsidiaries Otis Elevator Co. ("Otis") and Pratt & Whitney ("Pratt") made improper payments and provided other improper benefits to government officials in Azerbaijan, China, Kuwait, Russia, Pakistan, South Korea, Thailand, and Indonesia.

In Azerbaijan, the SEC Order alleges that an Otis affiliate in Russia ("Otis Russia") engaged in various schemes to sell elevator equipment to Baku Liftremont, a municipal entity in Azerbaijan. In one such scheme, Otis Russia allegedly used two subcontractors to make payments to Liftremont officials. Otis Russia paid the subcontractors nearly $800,000 (roughly 44% of the total contract value) without appropriate documentation or any due diligence. The SEC alleged that documentation failed to establish that the subcontractors provided services to justify the compensation. In another scheme, Otis Russia engaged a series of intermediaries as distributors, offering equipment at one price while knowing that the intermediaries would sell the equipment to Liftremont at an inflated price and use the difference to pay bribes to Liftremont officials. No due diligence was performed on the intermediaries, and they were engaged without business justification; Otis Russia's JV partner was already authorized to sell products in Azerbaijan. Through these and other schemes, the SEC Order alleges that Otis Russia entered into ten contracts with Liftremont with a total value of $14.6 million.

In China, Pratt and a Pratt joint venture, International Aero Engines ("IAE"), allegedly engaged in various corrupt schemes to sell airplane engines to Chinese state-owned commercial airlines, including Air China Ltd. In 2006, at the direction of Pratt, IAE retained a Chinese sales agent to help increase market share. Neither Pratt nor IAE conducted due diligence on the agent, who had no experience in the airline industry (the agent had previously worked in the toll road business). According to the Order, from 2009 to 2013, IAE paid the agent approximately $55 million in commissions. The SEC alleged that a portion of these commissions were passed on to officials at Chinese state-owned airlines in return for contracts. The SEC also alleged that IAE and Pratt used improper sponsorships to curry favor with Chinese officials. For example, in 2009 and 2011, IAE and Pratt contributed $30,000 each for a golf event for senior executives of a Chinese airline. At the event, expensive gifts, such as iPads and luggage, were provided by IAE's Chinese agent to the Chinese officials.

The SEC Order also highlighted allegedly improper leisure travel provided by UTC for foreign officials in China, Kuwait, South Korea, Pakistan, Thailand, and Indonesia. According to the SEC, UTC, through Pratt and Otis, frequently used trips and entertainment to reward or influence foreign officials. Employees allegedly sometimes circumvented UTC controls by submitting expenses for travel of foreign officials without disclosing the leisure aspect of the travel. The SEC faulted the legal department and supervisors for failing to identify red flags prior to approving these expenses. For example, the SEC noted that official travel for foreign officials to Orlando was approved despite the fact that Pratt did not have a facility there (and that it is a popular tourist destination). In other instances, UTC allegedly provided improper leisure travel in conjunction with legitimate business travel. In some instances, the leisure portion of the trips was four times as long as the business portion. In total, the SEC

alleged that between 2009 and 2015, UTC recorded $134,000 in improper travel and entertainment for foreign officials as legitimate business expenses.

In accepting the offer of settlement, the SEC took into consideration that UTC self-reported the misconduct, cooperated fully with the SEC's investigation, and engaged in extensive remedial measures, including the termination of employees and third parties involved in the misconduct.

20. Vantage Drilling International

Key Facts:

Agencies: SEC
Countries Involved: Brazil
Amount of Total Financial Settlement: $5 million
Means of Corruption: Agents

On November 19, 2018, Vantage Drilling International ("Vantage"), a NYSE-listed offshore drilling contractor based in Houston, Texas consented to the entry of an SEC issued a cease and desist order alleging that Vantage's predecessor, Vantage Drilling Company ("VDC"), violated the FCPA's internal accounting control provisions in connection with transactions involving a Taiwanese shipping magnate, Hsin Chi Su. Without admitting or denying the allegations, Vantage agreed to pay a penalty of $5 million for failing to maintain adequate internal accounting controls. The Department of Justice declined to prosecute Vantage in connection with the same conduct.

According to the SEC, in early 2007, VDC identified Su as a prospective investor and supplier of offshore drilling rigs as part of a strategy to expand VDC's oil and gas operations into the ultra-deep drilling market. VDC entered into a contract with Su in which VDC would acquire an ultra-deepwater drillship owned by Su—the *Titanium Explorer*—to be delivered in 2012. In exchange, VDC appointed Su to its board of directors, paid him $56 million in cash, and issued 40% of VDC's common stock to him, making him VDC's majority shareholder. The SEC alleged that VDC did not conduct any due diligence on Su in connection with the *Titanium Explorer* transaction.

The SEC alleged that, following the acquisition of the *Titanium Explorer*, VDC sought to market the *Titanium Explorer* to Petrobras, the Brazilian state-owned oil and gas giant. VDC's chief executive officer contacted a third-party agent to assist in this marketing effort. The agent learned that a senior Petrobras official was willing to accept a payment in exchange for awarding VDC the drillship contract. Part of this payment would be kept by the Petrobras official responsible for negotiating the contract and part would be provided to Brazilian politicians responsible for appointing the Petrobras official to his position. The agent contacted Su to arrange for him to provide the funds to make the payment to the Petrobras official.

According to the SEC, Su signed "consulting agreements" to formalize the payments, arranging to pay the agent in installments totaling $31 million. In February 2009, Petrobras and VDC entered into a $1.8 billion contract for the sale of the *Titanium Explorer* to Petrobras. As part of the transaction, VDC agreed to transfer all revenues received from Petrobras to Su, less VDC's management fee.

The SEC alleged that during the same time period, VDC sought to purchase a second ultra-deepwater drillship—the *Platinum Explorer*—from Su. Su represented to VDC that he was unable to make a $32 million installment to the shipyard engaged to construct the *Platinum Explorer*. VDC provided these funds to Su to facilitate the payment, but later learned that the $32 million was not yet due to be paid to the shipyard. The SEC alleged that despite learning about Su's misrepresentations regarding the *Platinum Explorer* installment, VDC nevertheless engaged in transactions that resulted in Su receiving revenues from the *Titanium Explorer* transaction.

In August 2015, citing a breach of obligations, Petrobras cancelled the *Titanium Explorer* contract, causing VDC to restructure its debt and transfer its assets to Vantage. An international arbitration ensued and a tribunal has since issued an award in favor of Vantage Deepwater Company and Vantage Deepwater Drilling, Inc., two wholly owned subsidiaries of Vantage, for over $700 million. According to the tribunal, the evidence presented was insufficient to establish that Vantage knew of the alleged payments, and therefore, that Petrobras cancelled the deal prematurely.

The SEC's order states that VDC ignored several red flags that indicated the improper payments to Petrobras officials. For example, an outside consultant suggested to VDC's chief executive officer that Su expected VDC to reimburse him for his "payment to P." A reporter also alerted the chief executive officer and marketing department that she was working on a story about alleged improper payments by Su to Petrobras to secure the *Titanium Explorer* contract.

The improper payments were exposed in 2015 as part of the sprawling investigation of Petrobras known as Operation Car Wash. Both Su and the agent who facilitated the *Titanium Explorer* contract were charged criminally in Brazil for their participation in wide ranging schemes to bribe Petrobras officials and Brazilian politicians.

The SEC asserted that VDC failed to establish and maintain sufficient internal accounting controls in connection with transactions with Su, particularly given the high risk associated with conducting business in the oil and gas industry in Brazil. VDC also allegedly failed to conduct due diligence on the agent and address red flags that Su and the agent paid bribes to secure the *Titanium Explorer* contract. In determining the penalty to impose for the alleged misconduct, the SEC considered Vantage's financial condition, its voluntary disclosure of information obtained during an internal investigation, and steps taken by Vantage to address the internal accounting failures identified by the SEC, including overhauling its board of directors and senior management.

Chapter 3:
U.K. Anti-Bribery Developments

I shall have jurisdiction in respect of corruption committed by those corporates anywhere in the world even if the corruption is not taking place through the business presence of the corporate in this jurisdiction.

- Richard Alderman, then-Director of SFO

I. Overview

On April 8, 2010, the House of Commons passed legislation to consolidate, clarify and strengthen the U.K. anti-bribery law. The Bribery Act creates four categories of offenses: (i) offenses of bribing another person; (ii) offenses related to being bribed; (iii) bribery of foreign public officials; and (iv) failure of a commercial organization to prevent bribery. The first category of offenses prohibits a person (including a company as a juridical person) from offering, promising, or giving a financial or other advantage: (a) in order to induce a person to improperly perform a relevant function or duty; (b) to reward a person for such improper activity; or (c) where the person knows or believes that the acceptance of the advantage is itself an improper performance of a function or duty. The second category of offenses prohibits requesting, agreeing to receive, or accepting such an advantage in exchange for performing a relevant function or activity improperly.

The third category of offenses, bribery of foreign public officials, is the most similar to the FCPA. According to the Bribery Act's Explanatory Notes, Parliament intended for the prohibitions on foreign bribery to closely follow the requirements of the OECD Convention, to which the United Kingdom is a signatory. Under the Bribery Act, a person (again, including a company) who offers, promises, or gives any financial or other advantage to a foreign public official, either directly or through a third-party intermediary, commits an offense when the person's intent is to influence the official in his capacity as a foreign public official and the person intends to obtain or retain either business or an advantage in the conduct of business. In certain circumstances, offenses in this category overlap with offenses in the first category (which generally prohibits both foreign and domestic bribery). The MOJ Guidance, however, highlights that the offense of bribery of a foreign public official does not require proof that the bribe was related to the official's improper performance of a relevant function or duty. The overlap between the general bribery offenses and the offenses relating to bribery of foreign officials also allows prosecutors to be flexible, enabling them to bring general charges when a person's status as a foreign official is contested or to seek foreign official bribery charges when an official's duties are unclear.

Finally, and most significantly for large multinational corporations, the Bribery Act creates a separate strict liability corporate offense for failure to prevent bribery, applicable to any corporate body or partnership that conducts part of its business in the United Kingdom. Under this provision, a company is guilty of an offense where an "associated person" commits an offense under either the "offenses of bribing another person" or "bribery of foreign public officials" provisions in order to obtain or retain business or a business advantage for the company. An "associated person" includes any person who performs any services for or on behalf of the company, and may include employees, agents, subsidiaries, and even subcontractors and suppliers to the extent they perform service on behalf of the organization. While failure to prevent bribery is a strict liability offense, an affirmative defense exists where the company can show it had in place "adequate procedures" to prevent bribery.

The offense of failure to prevent bribery stands in contrast to the FCPA's standard for establishing liability for the actions of third parties, such as commercial agents. Whereas the FCPA's anti-bribery provisions require knowledge or a firm belief of the agent's conduct in order for liability to attach, the U.K. Act provides for strict liability for commercial organizations for the acts of a third party, with an express defense where the company has preexisting adequate procedures to prevent bribery. This strict liability criminal offense creates significant new hazards for corporations when they utilize commercial agents or other third parties. In effect, the actions of the third party will be attributable to the corporation, regardless of whether any corporate officer or employee had knowledge of the third party's actions. The affirmative defense places a great premium on having an effective compliance program, including, but not limited to, due diligence procedures. In the United States, the existence of an effective compliance program is not a defense to an FCPA charge, though the DOJ and SEC do treat it as one

of many factors to consider in determining whether to bring charges against the company, and the U.S. Sentencing Guidelines include it as a mitigating factor at sentencing.

The Bribery Act has several other notable differences from the FCPA, and in many ways, the U.K. law appears broader. Portions of the Act are applicable to any entity that carries on a business, or part of a business, in the U.K., whether or not the underlying conduct has any substantive connection to the U.K. As Richard Alderman, the then-Director of the Serious Fraud Office (SFO), the U.K. agency responsible for the investigation and prosecution of corruption and fraud, explained in a June 23, 2010 speech:

> I shall have jurisdiction in respect of corruption committed by those corporates anywhere in the world even if the corruption is not taking place through the business presence of the corporate in this jurisdiction. What this means is this. Assume a foreign corporate with a number of outlets here. Assume that quite separately that foreign corporate is involved in corruption in a third country. We have jurisdiction over that corruption.

Furthermore, the Bribery Act criminalizes bribery of private persons and companies in addition to bribery of foreign public officials. The Act also provides no exception for facilitation or “grease” payments, nor does it provide any exception for legitimate promotional expenses, although it is arguable that properly structured promotional expenses would not be considered as intended to induce a person to act improperly and therefore would not violate the Act.

On several occasions since the passage of the Bribery Act in 2010, authorities have issued guidance on the law’s interpretation and implementation. Below, we summarize the most recent of this guidance, the August 2019 SFO *Corporate Cooperation Guidance*. A full discussion of historical guidance and other relevant legislation can be found in our *Anti-Bribery Compendium*.

II. <u>SFO Corporate Cooperation Guidance</u>

In August 2019, the SFO issued a memo laying out steps that a company should take when cooperating with the SFO during an investigation. According to the guidance, cooperation requires companies to go “above and beyond what the law requires.” Cooperation includes identifying suspected wrongdoing and criminal conduct, along with the individuals responsible; reporting this suspected wrongdoing to the SFO within a reasonable amount of time; and preserving evidence and providing it promptly in an “evidentially sound format.”

The guidance also provides examples of actions that are “inconsistent” with cooperation, such as protecting certain individuals, wrongly blaming others, notifying individuals that they are the subject of an investigation (thereby creating a risk of tampering with evidence or altering testimony), and tactical delays or “information overloads.” It emphasizes that cooperation does not guarantee any specific outcome. It notes that cooperation with compulsory processes used by the SFO to obtain relevant material does not itself indicate cooperation, but equally caveats that use of compulsion as a means of obtaining materials does not necessarily indicate that the SFO considers the company to be non-cooperative.

The guidance provides examples of actions a company can take in various contexts that typically constitute cooperation. Generally, the SFO suggests:

- Preserving both digital and hard-copy material, and ensuring the integrity of material is preserved;

- Providing the material (including material held overseas but under the control of the company) promptly and in a structured way, with a list of custodians and locations of the documents;
- Promptly informing the SFO of any suspected data loss, deletion, or destruction;
- Identifying material that is in the possession of third parties and facilitating the production of this material;
- Assisting in identifying material that might be capable of helping any accused or undermining the case of prosecution; and
- Promptly providing a schedule of documents withheld due to privilege and the basis for the assertion of privilege.

If the company claims privilege, it must establish a valid privilege claim, including providing certification by outside counsel that the material in question is privileged. A company that chooses not to waive privilege and provide fact witness accounts will not be penalized by the SFO for this decision, but will not earn cooperation credit as a factor weighing against prosecution under the Deferred Prosecution Agreements Code (*see above*). Further, the SFO notes in the guidance that, even when a company decides not to waive privilege, the SFO still has obligations to potential individual defendants to disclose certain materials.

The guidance provides specific suggestions on how to handle both digital and hard-copy evidence. For digital material, suggestions include producing the evidence in a format that it is ready for review; creating an audit trail of the acquisition of the data and devices; alerting the SFO to information it cannot access; and preserving passwords, recovery keys, decryption keys, and other data necessary to review the digital devices. Similarly, hard-copy or physical evidence and financial records should be accompanied by an audit trail of the acquisition and handling of that evidence, and corporations should "identify a person to provide a witness statement covering continuity."

The guidance also provides suggestions for handling financial records and analysis. Generally, companies should provide records showing the flow of relevant funds, along with organizational financial records including bank records, invoices, money transfers, and other similar documents (produced in a structured way). Companies should alert the SFO to relevant financial material that the company cannot access, and should ensure that accountants are available to produce and explain the financial records. Finally, companies should also provide financial information relevant to profit, disgorgement, and financial penalty calculations, as well as to the company's ability to pay.

Further, the SFO's guidance lists best practices for a target company's interactions with relevant individuals. A company should consult with the SFO before interviewing potential witnesses or suspects and must refrain from tainting a potential witness's testimony. For example, a company should not share one person's account with another or show the witness documents that were not previously available to the witness. Companies should make employees and agents available for SFO interviews, provide last-known contact information of former employees or agents, and identify potential third-party witnesses. In the event that a company conducts interviews as part of an internal investigation, the company should provide witness accounts, as well as any recordings, notes, or transcripts of the interviews.

Finally, the guidance indicates that a cooperative company should provide the SFO with industry knowledge, context, and common practices, as well as potential defenses that are typical in the industry. A company

cooperating with the SFO should provide information on other actors, and notify the SFO of any other government agency that has been in contact with the company or to whom the company reports.

III. Legal Privilege and Data Gathering Developments in the U.K.

As the SFO continues to mature and becomes increasingly active, companies subject to potential or actual SFO investigations should pay close attention to the rapidly evolving landscape of U.K. legal privilege as laid out in recent case law, and should be aware of recent developments designed to enhance the ease with which U.K. authorities gather information on targets of investigations.

A. SFO v. Eurasian Natural Resources Corporation

On May 8, 2017, Justice Andrews of the High Court of Justice, Queen's Bench Division, handed down a decision in *Serious Fraud Office v. Eurasian Natural Resources Corporation* presenting a restrictive interpretation of both forms of legal privilege in the U.K., litigation privilege and legal advice privilege, as applied to documents created during an internal investigation. On September 5, 2018, however, Eurasian Natural Resources Corporation ("ENRC") prevailed in its appeal of this decision with the Court of Appeal, which overturned in large part Justice Andrews's analysis and held that litigation privilege protected the contested documents.

The dispute originated as part of the SFO's criminal investigation into alleged fraud, bribery, and corruption by ENRC. In August 2011, ENRC engaged outside counsel to conduct an internal investigation into a whistleblower's allegations of corruption in ENRC's wholly-owned Kazakh subsidiary. It later directed the law firm to conduct a second investigation, this time into allegations of impropriety surrounding ENRC's acquisition of a mine in Africa. The investigations, which ran until April 2013, occurred simultaneously with a dialogue between ENRC and the SFO regarding the various allegations. That dialogue broke down—and the SFO commenced a formal criminal investigation—when ENRC dismissed the law firm conducting the internal investigations and liaising with the SFO on ENRC's behalf.

During the course of its investigation, the SFO sought to compel ENRC to produce documents primarily generated by outside counsel and forensic accountants during the course of the internal investigation. The documents included, among other things, notes taken by outside counsel during investigative interviews. ENRC refused to produce the documents, claiming they were protected by legal advice privilege, litigation privilege, or both. The SFO then brought the matter before the court. Justice Andrews sided with the SFO and, with the exception of slides prepared by ENRC's counsel for presentation to the Board of Directors, determined that the documents were not protected by legal advice privilege.

With respect to litigation privilege, Justice Andrews held that simply anticipating a criminal investigation by the SFO fails to fulfill the requirement that adversarial litigation be reasonably in contemplation, stating that "prosecution only becomes a real prospect once it is discovered that there is some truth in the accusations, or at the very least that there is some material to support the allegations." Further, litigation privilege only holds if the documents were produced predominantly for the purpose of conducting adversarial litigation. In this case, the court found, the documents at issue were produced first as part of a fact-finding mission, and then in connection with advice about how to reach a civil settlement—in other words, to avoid litigation, rather than to conduct it.

Concerning legal advice privilege, Justice Andrews held that the only documents falling under the umbrella of protection were a set of slides prepared by ENRC's counsel for presentation to the Board of Directors on the Board's request for legal advice. The court found no evidence that the remaining documents summarized legal advice for individuals authorized by ENRC to seek it. Further, it held that the underlying communications were not privileged, because they were not made for the purpose of instructing counsel on behalf of the company. Justice

Andrews specifically rejected the contention that a document can be privileged simply by virtue of being drafted by an attorney: “A document . . . that would not be privileged if it had been created by a non-lawyer does not acquire a privileged status just because a lawyer has created it.”

In a decision that has been widely applauded by the legal community, the Court of Appeal overturned much of the High Court’s decision, largely restoring legal privilege protection to internal investigations conducted by counsel. With regard to litigation privilege, the Court of Appeal held that anticipating a criminal investigation fulfills the requirement that adversarial litigation is reasonably in contemplation. The Court of Appeal held that the lower court was wrong to find that there is a general principle that litigation privilege does not attach in the context of internal investigations until either a company knows the full details of what is likely to be unearthed by the investigation or a decision to prosecute has been made. The Court of Appeal also found that the evidence demonstrated that the documents at issue were created for the dominant purpose of resisting the contemplated criminal proceedings, and that it was of no issue that ENRC considered sharing materials from its investigation with the SFO as part of its negotiation strategy.

The Court of Appeal did not reach a decision on the question of whether the internal investigation documents may have also been protected under the legal advice privilege because it found that they were protected by the litigation privilege. Although the Court of Appeal largely agreed with the High Court on legal advice privilege, finding that under current English law the privilege only covers information received by counsel from ENRC or personnel authorized to seek or receive legal advice, the Court of Appeal noted that it would favor a more expansive interpretation that would include lawyers’ communications with employees of the client that were not directly authorized to seek or receive legal advice. According to the Court of Appeal, such a broader definition would better meet the practical realities of multinational companies and should therefore be considered by the U.K.’s Supreme Court or by the Court of Appeal in an appropriate case.

B. U.S.-U.K. Bilateral Data Access Agreement

On October 3, 2019, the U.S. and U.K. entered into the U.S.-U.K. Bilateral Data Access Agreement (the “Agreement”), which removes legal barriers to gathering electronic information in an effort to promote the access and collection of data for criminal investigations in both countries. The Agreement is the first of its kind under the U.S. Congress’s Clarifying Lawful Overseas Use of Data Act (“CLOUD Act”), which was passed in 2018.

Under the Agreement, each country will lift certain restrictions that prohibit companies from complying with information requests that come from authorities in the counterparty country. However, authorities in both countries also emphasized that the new procedures for requesting data will be governed by safeguards meant to protect civil liberties and individual rights under both countries’ legal systems. Requests are limited to “serious crimes,” as defined by the requesting country, and cannot target residents of the other country. Further, each country committed to obtain permission from the other country before using data gained from the agreement in prosecutions relating to a party’s “essential interest”—in the United States, charges that may carry the death penalty, and in the U.K., charges that implicate freedom of speech.

The Agreement will enter into force after a six-month U.S. Congressional and U.K. Parliamentary review, and will last for five years barring any changes or extensions agreed upon by both parties. U.K. Home Secretary Priti Patel stated that the Agreement is expected to “dramatically” increase the speed of criminal investigations. She noted that currently, prosecutors in the U.K. wait up to two years before they are able to access U.S.-held data. The Agreement is likely to provide some measure of relief to the SFO, which has come under criticism recently for the speed at which its corruption investigations are proceeding.

IV. U.K. Investigations and Enforcement Actions

Despite the legislation permitting deferred prosecution agreements and subsequent guidance on their use, the SFO offers DPAs on a selective basis, having resolved only five matters through DPAs since Parliament authorized their use in 2013. However, the agency does continue to open and conduct investigations into suspected corruption by both corporations and individuals. Below, we summarize a selection of recent U.K. enforcement actions and updates to enforcement actions of note, as well as recently announced investigations, organized by the date of the action announced or taken against the corporate entity in question. For discussion of historical U.K. enforcement actions and investigations, please see the *HHR Compendium*.

A. Recent Enforcement Actions and Updates of Note

1. Alstom

On July 23, 2019, the U.K. Court of Appeal's Criminal Division upheld Alstom Network U.K.'s April 10, 2018 conviction for conspiracy to corrupt arising from a bribery scheme to obtain a construction contract in Tunisia. Following the conviction, Alstom appealed, arguing that the absence at trial of the individuals responsible for the corrupt scheme precluded a fair trial. The Court of Appeal rejected this argument, noting that Alstom "participated effectively" in the trial and declining to adopt the interpretation that a corporate conspirator cannot be tried without the presence of responsible individuals. Alstom Network U.K. is now awaiting sentencing.

Separately, three former Alstom employees have been sentenced for their roles in a bribery scheme to secure power contracts in Lithuania worth EUR 240 million. On December 21, 2018, the Global Sales Director for Alstom Power Ltd.'s Boiler Retrofits, Nicholas Reynolds, was sentenced to four years and six months' imprisonment and ordered to pay £50,000 in costs. Reynolds, who was found guilty by a jury of conspiracy to corrupt on December 19, 2018, is appealing his conviction. On July 9, 2018, the Regional Sales Director at Alstom Power Sweden AB, Göran Wikström, was sentenced to two years and seven months' imprisonment following his June 22, 2018 guilty plea of one count of conspiracy to corrupt. Finally, on May 4, 2018, the Business Development Manager at Alstom Power Ltd., Johanes Venskus, was sentenced to three years and six months' imprisonment following his October 2, 2017 guilty plea of one count of conspiracy to corrupt.

The SFO first announced an investigation into Alstom's U.K. subsidiaries on June 18, 2009, and its investigation remains ongoing. A full description of the Alstom matter can be found in the *HHR Compendium*.

2. Sarclad Ltd.

On July 16, 2019, the SFO determined that Sarclad Ltd ("Sarclad") had met the terms of its July 11, 2016 DPA, and the agreement between the parties concluded. Under the terms of the agreement—which was only the SFO's second DPA—Sarclad, then referred to as "XYZ Ltd." To preserve the company's anonymity, agreed to pay £6,201,085 in disgorgement of gross profits and a £352,000 financial penalty to the SFO for violations of the Bribery Act 2010 and the Criminal Law Act 1977. At the time of the final approval of the judgment, the Crown Court indicated that there were related ongoing criminal proceedings against undisclosed parties, and that Sarclad's identity would ultimately be disclosed at the termination of those proceedings and when the disclosure would not be contrary to the interest of justice. A full description of the Sarclad matter and related individual prosecutions can be found in our *Anti-Bribery Compendium*.

3. Serco Geografix Ltd. and Serco Group

On July 4, 2019, the SFO announced that it received final approval to enter into a DPA with Serco Geografix Ltd. ("SGL"), a company that provided electronic monitoring services for the Ministry of Justice. SGL's crimes arose from a false accounting scheme to deliberately mislead the Ministry of Justice regarding how much SGL's immediate parent company, Serco Limited, profited from the contract between 2010 and 2013. By deceiving the Ministry of Justice, SGL prevented the Ministry from seeking more favorable terms during contract negotiations. The issue was first reported to SFO by Serco Limited itself in 2013.

Under the DPA, SGL must cooperate with the SFO and other foreign and domestic enforcement and regulatory authorities, self-report any evidence of fraud by itself or related entities, and enhance its ethics and compliance regime. In addition, the DPA is accompanied by a formal undertaking by Serco Group, SGL's and Serco Limited's ultimate parent company, to cooperate with the same authorities, report fraud by itself or related individuals, and strengthen Group-wide ethics and compliance functions. The DPA and associated obligations are in effect for a period of three years.

This is the SFO's fifth DPA and its first "group" DPA that is accompanied by an agreement imposing conditions on the parent company as well as the subsidiary. In addition to the obligations noted above, SGL agreed to pay £19.2 million in fines and £3.7 million in costs.

4. F.H. Bertling Ltd. and Related Individuals

On June 3, 2019, the SFO announced that F.H. Bertling Ltd. ("Bertling"), a U.K.-based provider of logistics and project freight operations, would be fined £850,000 in connection with its August 1, 2017 guilty plea for its part in a multi-year scheme to bribe an agent of Angola's state-owned oil company. This fine is the latest development in a series of actions the SFO has taken against Bertling and several individuals in connection with making, and conspiring to make, corrupt payments related to freight forwarding contracts in Angola and the North Sea. These actions are the product of an investigation that began in September 2014. A full description of the Bertling matter can be found in our *Anti-Bribery Compendium*.

5. Standard Bank PLC

On November 30, 2018, the SFO found that Standard Bank had complied fully with the terms of its November 30, 2015 DPA—the SFO's first—and the agreement between the two concluded. The DPA arose from conduct by Standard Bank's former sister bank, Stanbic Bank Tanzania, which paid $6 million to Enterprise Growth Market Advisors to induce Tanzanian officials to select Standard Bank to lead a $600 million private placement for the Government of Tanzania. This private placement generated $8.4 million in fees for Standard Bank. Under the DPA, Standard Bank was required to pay a penalty of $25.2 million and a further $7 million in compensation to the Government of Tanzania. It also agreed to pay £330,000 in costs to the SFO, continue to cooperate fully with the SFO, and implement the recommendations of an independent auditor in exchange for the suspension of the indictment.

6. Unaoil Group

On June 26, 2018, the SFO charged Unaoil Group ("Unaoil") companies Unaoil Ltd. and Unaoil Monaco SAM each with two counts of conspiracy to give corrupt payments in connection with alleged bribery schemes to secure the award of contracts in Iraq. The accusations against Unaoil Ltd. relate to a $733 million oil pipeline contract in southern Iraq awarded to Leighton Contractors Singapore PTE, while those against Unaoil Monaco

SAM relate to contracts in Iraq awarded to Unaoil client SBM Offshore. These charges arise out of an SFO investigation that began in March 2016.

In addition to taking action against corporate Unaoil entities, the SFO has also charged a number of individuals related to Unaoil for their roles in the alleged bribery schemes. In relation to the award in Iraq of contracts to SBM Offshore, Basil Al-Jarah (Unaoil's Iraq partner), Ziad Akle (Territory Manager for Iraq, Unaoil), Paul Bond (Senior Sales Manager, SBM Offshore), and Stephen Whitely (Vice President, Unaoil) have been charged with conspiracy to give corrupt payments. Messrs. Al-Jarah and Akle have also been charged with conspiracy to give corrupt payments in connection with the award of the $733 million contract to Leighton, and in December 2018, the SFO charged Mr. Whiteley with another count of conspiracy to make corrupt payments arising out of Whiteley's alleged assistance to ensure the engagement of Unaoil Ltd. as a subcontractor for an Iraqi oil pipeline project.

In July 2019, Al-Jarah pleaded guilty to five charges of conspiracy to give corrupt payments arising out of the award of contracts to supply and install mooring and oil pipelines in southern Iraq. The remaining defendants are scheduled to begin trial on January 13, 2020.

Separately, the SFO also requested the extradition of Saman Ahsani, one of Unaoil's owners, from Monaco, but this request was denied in a final decision by authorities in Monaco in March 2018 because the alleged acts did not constitute a crime under Monégasque law at the time they were committed. Media reports indicated that the SFO's investigation into Ahsani and Unaoil's remaining two owners was halted in June 2019.

Certain media outlets also reported that the SFO terminated its investigation into Unaoil itself in June 2019, though the SFO continues to list Unaoil among its active investigations as of October 2019.

A number of other SFO investigations and internal investigations relate to the Unaoil matter. Two of these, KBR Inc. and Petrofac PLC, are discussed under *Recent Investigations*, below. The remainder are summarized in our *Anti-Bribery Compendium*.

B. Recent Investigations

1. Guralp Systems Ltd.

On August 17, 2018, the SFO announced an investigation into Guralp System Ltd., a manufacturer of seismometers, for allegedly engaging in corrupt actions in connection with the sale of seismic equipment to the Korea Institute of Geoscience and Mineral Resources ("KIGAM"). Guralp's founder, Cansun Guralp, and an employee, Andrew Bell, were also arrested and charged with conspiracy to make corrupt payments. On September 28, 2018, Natalie Pearce, Guralp's former sales director, was similarly charged with conspiracy to bribe a foreign official. In 2017, KIGAM's former director was sentenced to 14 months in federal prison in the United States for using a Southern California bank account to launder bribes that he received from two unnamed seismological companies (See "Heon Cheol Chi" in the *HHR Compendium*). The investigation into Guralp Systems Ltd. Remains ongoing as of October 2019.

2. Petrofac PLC

On May 12, 2017, the SFO announced that it had opened an investigation into U.K. oilfield services company Petrofac PLC ("Petrofac"), its subsidiaries, and related individuals for suspected bribery, corruption and money laundering, noting that this investigation was related to the Unaoil probe. Petrofac had retained Unaoil for consulting services, primarily in Kazakhstan, from 2002 to 2009.

In a May 25, 2017 press release, Petrofac announced that it had suspended its COO, Marwan Chedid, and that CEO Ayman Asfari would not take part in any matters related to the investigation. Both were arrested but subsequently released without charge. Petrofac also disclosed that in 2016 its board had commissioned an investigation into the Unaoil-related allegations, that it had turned over the results to the SFO, and that the SFO did not accept the findings of the internal investigation. On August 9, 2017, Petrofac announced that it had appointed an outside attorney to serve in an oversight role with respect to the SFO investigation.

On February 6, 2019, Petrofac International Limited's former Global Head of Sales, David Lufkin, pleaded guilty to eleven counts of bribery related to making corrupt offers to influence the award of $730 million in Iraqi contracts and $3.5 billion in Saudi contracts to Petrofac. According to the SFO's description of the charges, Lufkin was involved in paying $2.2 million via two agents in return for a $329.7 million Engineering, Procurement, and Construction contract on the Iraqi Badra oilfield; making additional corrupt offers of payment via an agent to influence the award of other Badra-related contracts; paying $4 million via an agent for a $400 million operations and maintenance contract on the Iraqi Fao Terminal; and making $45 million in corrupt payments for a series of Saudi contracts also related to the oil projects.

On August 4, 2019, the SFO accused four senior managers at Petrofac, George Salibi, E.S. Sathyanarayanan, Mani Rajapathy, and Paolo Bonucci, of working with Lufkin to pay multimillion-pound bribes in exchange for contracts. These cases remain pending as of October 2019.

3. KBR, Inc.

On April 28, 2017, the SFO announced that it had opened an investigation into KBR Ltd., the United Kingdom subsidiary of American engineering and construction company KBR, Inc. ("KBR"), and related individuals for suspected bribery and corruption, noting that this investigation was related to the Unaoil probe. KBR issued a press release indicating that it had launched an internal investigation into the matter, and that it would cooperate with the SFO, as well as with the DOJ and SEC, which are also conducting investigations into "the same facts and circumstances."

In an April 2018 judicial review hearing by the U.K. High Court, KBR objected to a document production request presented to it by the SFO, arguing, *inter alia*, that the SFO did not have extraterritorial reach to compel production by the U.S. parent for documents located in the United States. KBR argued that the SFO should instead seek those documents through Mutual Legal Assistance Treaty procedures. It further objected to the manner of service effectuated by the SFO, which was at a meeting at the SFO with KBR Ltd. in the United Kingdom at which the SFO had insisted that someone from KBR, Inc. also be present. KBR argued that the transient presence of the corporate secretary in the United Kingdom did not imply that KBR was amenable to service there.

That same month, the president of KBR's oil and gas business, Jan Egil Braendeland, was arrested as part of the SFO's investigation into KBR. However, he was not charged with an offense and was released shortly thereafter.

On September 6, 2018, the High Court ruled that a non-U.K. corporation could be compelled to produce documents that were outside the country if there was a "significant connection" with the United Kingdom. Whether such a connection exists is a fact-specific inquiry not satisfied solely by a parent-subsidiary relationship. However, in this case, the court ruled that the standard was met, noting KBR's role in approving and processing a number of suspect payments from KBR Ltd. to Unaoil, as well as KBR's generally close involvement in KBR Ltd.'s operations. Furthermore, the High Court ruled that document production notices served under the authority of Section 2 of the Criminal Justice Act 1987 (such as the SFO's notice to KBR) are not subject to the Civil

Procedure Rules on service and that the SFO's provision of the notice to KBR's corporate secretary therefore was sufficient—although the court did note that the process used by the SFO to insist on KBR's presence at a meeting was "unappealing."

On April 6, 2019, the U.K. Supreme Court granted KBR leave to appeal the lower court's decision. As of October 2019, the Supreme Court had yet to issue its ruling.

Chapter 4: Anti-Corruption Enforcement Update - France

France's rapidly evolving regulatory environment sets it up to become a major player in the fight against global corruption. It also creates challenges and requires careful attention from French companies.

As with many OECD signatories, France has faced criticism regarding its lack of enforcement of foreign corruption cases. It has taken these critiques to heart and, in 2016, instituted sweeping changes to its anti-corruption legal framework in order to require certain companies to develop and maintain corporate compliance programs that can prevent and detect corrupt practices. France has also passed laws that seek to impose other ethical practices on French companies. The following section will examine France's evolution in the anti-corruption landscape, how these practices affect companies working in France, and how the anti-corruption regulatory regime is likely to develop.

I. Sapin II

Under international pressure to comply and implement its obligations under the OECD Convention on Combating Bribery of Foreign Officials in International Business Transactions ("OECD Convention"), and a desire to ensure that corruption matters were handled by French (as opposed to non-French regulators), France enacted a series of reforms targeting corrupt activities and promoting transparency. The most significant of these to date is Act No. 2016-1691, entitled "Transparency, the Fight against Corruption and the Modernization of the Economy" (named after then-Minister of Finance, Michel Sapin, hereinafter "Sapin II"). As part of these reforms, France: (i) criminalized the peddling of influence of foreign officials; (ii) extended French jurisdiction over certain corruption related offenses; (iii) created an instrument whereby companies could negotiate corporate resolutions (similar to a deferred prosecution agreement); (iv) created the Agence française anticorruption (French Anticorruption Agency, or "AFA"); (v) required companies of a certain size to adopt and implement anti-corruption compliance programs; (vi) introduced a new criminal penalty in the form of an imposed monitorship by the AFA; (vii) provided additional protections for whistleblowers; and (viii) imposed an obligation to disclose certain affiliations with lobbyists.

A. Criminalization of the Influence Peddling of Foreign Officials

Prior to the adoption of Sapin II, "influence peddling" (*trafic d'influence*) of public officials – or the offering or solicitation of an improper advantage by a public official or a person vested with a public service mandate in order to use his or her apparent or actual influence in order to obtain undue favors or treatment – was punished only if carried out with respect to French officials, or officials of public international organizations (such as the United Nations). Under Sapin II, the offenses of active and passive influence peddling have been extended to include foreign government officials. Persons found guilty of influence peddling face penalties of up to five years imprisonment and a maximum criminal fine of 500,000 € or double the proceeds of the offense (whichever is the greater), bearing in mind that criminal fines against companies can be multiplied by up to five times those against natural persons (which would amount to penalties of up to 2.5 million €).

B. Extension of French Jurisdiction Regarding Corruption Offenses

Sapin II extended the extraterritorial reach of French anti-corruption law in two significant ways. First, it removed certain procedural requirements that previously limited prosecutors' ability to prosecute foreign corruption cases. Under French law, criminal offenses that occur abroad are typically subject to a "dual criminality" requirement. In other words, to be punishable in France, the conduct, which occurred overseas, must represent a criminal offense under the laws of France *and* the country where it occurred. Sapin II removed this requirement for acts of public corruption and influence peddling, meaning that such acts can be prosecuted in France regardless of whether they constitute a criminal offense in the country in which the conduct took place.

Sapin II also extended the application of French criminal laws regarding corruption and influence peddling to encompass any defendant that conducts part or all of its business in France. Consequently, under Sapin II,

corruption and influence peddling laws apply to all instances where the defendant is a French national, ordinarily resides in France, or conducts part or all of its business in France.

Another result of Sapin II is that the prosecutors no longer have the exclusive right to initiate prosecution or action against a company for alleged bribery of a foreign public official. Now, potential victims of the offense may also trigger prosecution by filing a complaint with the investigative magistrate. This expansion of the right to initiate action in such cases is already being tested in practice, with certain civil society organizations (such as for example Anticor, Transparency International France and Sherpa) bringing civil claims for alleged corrupt conduct.

The extension of victim's standing and rights to initiate action – both in terms of the prosecutors' extraterritorial reach in corruption cases and the potential for suits brought by civil society organizations – may prompt prosecutors to take a more active role in investigating and enforcing foreign bribery violations. If such an increase was meant to address the OECD's recommendations, preparatory steps under the law illustrate that it was also designed to align the scope of French anti-corruption laws with those of other jurisdictions, such as the U.S. Foreign Corrupt Practices Act and the U.K. Bribery Act.

C. Creation of a "French DPA" - La Convention Judiciaire d'Intérêt Public

1. Background

Implemented as part of Sapin II, the "judicial settlement of public interest" (Convention judiciaire d'intérêt public or ("CJIP")) is considered to be a major breakthrough in contemporary French anti-corruption law and provides French prosecuting authorities with tools more aligned with their foreign counterparts. It was also one of the most debated elements of Sapin II. The primary criticisms were that such a mechanism favors a financial transaction over the defense of the public interest, that it prevents public debate and excludes the victim from the settlement, and that it is reserved for companies and not applicable to individuals. After having been abandoned from the draft bill, the CJIP was reintroduced and reshaped to address certain aspects of these criticisms. Eventually adopted, the CJIP, which was inspired by deferred prosecution agreements ("DPAs") already used in the U.S. and U.K., is aimed at aligning France with these foreign counterparts and allowing faster and more efficient resolutions for companies.

Since its implementation in the French legal framework in 2016, seven companies have agreed to pay the fine provided for in a CJIP rather than taking the risk of being tried in court. In the absence of formal directions in the law as to how to conclude or implement a CJIP, the outcomes of these seven CJIPs combined with both (i) the circular issued by the Ministry of Justice on January 31, 2018 ("the Circular") and (ii) the guidelines issued jointly on June 29, 2019 by the *Parquet National Financier* and the AFA ("the PNF/AFA Guidelines") provide some insight on the main aspects. It is worth noting that both the precedents and the guidelines only provide general insight into how prosecutors are likely to handle the negotiation of a CJIP and cannot be considered as binding on companies or prosecutors in all circumstances.

2. Material and Personal Scope

Offenses eligible for a CJIP. CJIPs were initially only available in cases that could be characterized as offences of corruption, influence peddling, and/or laundering of the proceeds of tax fraud and related offences. Since the enactment of the Anti-Fraud Act on October 23, 2018, however, CJIPs are also available in cases of tax fraud.

Persons eligible for a CJIP. The CJIP provides corporations (even those below the financial and personnel thresholds established by Sapin II) with the possibility to settle certain criminal cases outside of the courtroom. Importantly, this alternative negotiated resolution mechanism is available only for legal entities and not for

individuals. Hence, the potential benefits of the CJIP do not extend to the companies' representatives and employees, who remain subject to prosecution even though a settlement agreement is entered into by the legal entity. However, the Parquet National Financier publicly stated that the plea agreement procedure (comparution sur reconnaissance préalable de culpabilité or ("CRPC")) could be available for individuals who agree to the alleged facts.

3. Content

Pursuant to the French Code of Criminal Procedure, a CJIP must include one or all of the following obligations: (i) the payment of a public interest fine that is to be proportionate to the gains obtained from the breach, without exceeding 30% of the entity's average annual turnover over the last three years; (ii) the implementation of a compliance program under the supervision of the AFA for a maximum of three years; and, (iii) the indemnification of any known victim, with payment having to be made within a year of the CJIP. CJIPs are required to contain a precise statement of facts and the legal characterization of such facts, but they do not require an admission of guilt.

4. Advantages of CJIPs

No admission of guilt. The CJIP has the effect of bringing an end to the prosecution against the legal entity without requiring any conviction or admission of guilt. As such, it does not entail debarment of the legal entity from national public procurement and makes it possible to continue to respond to calls for tenders related to international public contracts. It also avoids situations where the legal entity is prohibited from carrying on certain corporate activities, such as making a public offering, issuing financial securities in negotiations on a regulated market, or closing one or more of its establishments.

Reduced length of proceedings. The CJIP also has value for a legal entity in cutting the frequently very lengthy duration of proceedings and their uncertain nature, which can destabilize an organization's image, business activities and governance.

Foreseeability of costs. The CJIP provides the possibility to predict with greater certainty the fines and related costs that must be paid by the legal entity. Indeed, pursuant to Sapin II the payment of the public interest fine under a CJIP must not exceed 30% of the entity's average annual turnover on the last three years.

Reduced costs. While the Circular underlines that the settlement fine is to be higher than the amount that could be ordered in court – on the theory that a higher financial penalty is offset by the absence of a conviction and corresponding criminal record – the experience to date shows that in one instance, proposed penalties in the context of a CJIP negotiation were significantly lower than the fine eventually imposed by a court. Indeed, the CJIP offered to UBS to resolve a tax fraud case was reportedly rejected in March 2017 by the bank which considered the proposed fine, 1.1 billion €, to be excessive. In February 2019, UBS was sentenced after trial to pay a record fine of 3.7 billion € (plus 800 million € as damages). Given the limited experience offered so far, companies may be more incentivized (from a financial and risk management perspective) to enter into the CJIP process than risk such severe penalties after trial.

5. Risks associated with CJIPs

Lack of legal certainty. While Article 41-1-2 of the French Code of Criminal Procedure provides that "*if the president of the court does not validate the proposal of an agreement or if the legal entity avails itself of its right of retraction, the National Financial Prosecutor may not submit to the investigating judge or to the trial court*

declarations made or documents passed on by the legal entity in the course of the procedure described in this Article." It appears from the parliamentary debates that this was added to the law with the view to guarantee the confidentiality of the information disclosed by the legal entity, where the legal entity does not comply with the terms of the CJIP. Yet, the ambiguity surrounding the term "procedure" is also addressed by the PNF/AFA Guidelines. In particular, the PNF/AFA Guidelines state that the "procedure" (with the confidentiality obligations it carries) will not be initiated before the CJIP proposal has been formalized by the PNF. As such, the PNF/AFA Guidelines appear to take the view that it does not limit the prosecutors' ability to make use of the documents and information passed on by the company or its counsel at the criminal investigation stage (which is necessarily prior to formalization of a proposal for a CJIP). This position appears to conflict with the objective of inducing companies to spontaneously reveal to the prosecutor facts of corruption and/or influence peddling.

Questions regarding legal privilege. The PNF/AFA Guidelines take a more skeptical view of the applicability and importance of protections afforded by legal privilege (secret professionnel), and indicate that the level of the company's cooperation may be adversely affected by the refusal to transmit documents protected by the legal privilege. Companies therefore must balance the need and desire to communicate in a fulsome manner with their legitimate interest in maintaining legal privilege as well as their right against self-incrimination. In addition, companies that do consider waiving legal privilege protections must consider the effect of such a waiver in other jurisdictions.

6. Process

CJIP Proposition. The CJIP is to be offered at the initiative of the prosecutor or the investigative judge, depending on the current stage the prosecution. The prosecutor (not the AFA) may propose a settlement agreement for an implicated company as long as the company has not been formally charged ("[t]ant que l'action publique n'a pas été mise en movement") with the offence eligible for that type of resolution. Alternatively, when the case has been brought to the investigative magistrate (juge d'instruction) — which means that the public prosecution has already been initiated — the latter can decide to transmit the case to the prosecutor with the view to offer a CJIP to the company which has been indicted (mise en examen). Pursuant to the French Code of Criminal Procedure, an indicted company must acknowledge the alleged facts and agree to their proposed legal characterization in order to benefit from a CJIP.

In practice, however, the option to enter into a CJIP negotiation can also be suggested by the implicated company. Indeed, in most of the court validation orders issued to date, the judge noted that the CJIP resulted from the company's "clear and unequivocal" request to enter into negotiations with the prosecutor. This practice was recently endorsed by the PNF/AFA Guidelines, which states that a company wishing to suggest settlement negotiations does not have to formalize this into writing as, at this stage, the objective is only for the prosecutor to assess whether a negotiation can be considered.

Validation. Once the negotiations have started and after an agreement has been reached, the CJIP must be subject to judicial scrutiny, with the prosecutor proposing the draft settlement to the court. A public hearing is held, following which the judge decides whether or not to approve the settlement. This entails an assessment of whether the procedural requirements have been met, the substantive conditions, the amount of the fine, and the proportionality of the terms in light of the benefits derived from the violations. The decision cannot be appealed. If the court approves the settlement, the company has ten days to withdraw its acceptance. The approval order contains no finding of guilt and has neither the nature nor the effect of a conviction. The CJIP settlement, the approval order, and the amount of the fine are to be published on the AFA's website.

If the court does not approve the settlement, or if the company withdraws its acceptance/does not satisfy the terms of the agreement, the prosecutor then moves forward with the prosecution. If the court does not approve

the settlement or the company withdraws its acceptance, then the prosecutor cannot make use of statements made or documents provided by the company in the course of settlement discussions before an investigative magistrate or at trial. In contrast, the law does not guarantee confidentiality in the situation where a prosecution resumes because the company failed to comply with the requirements imposed by the CJIP.

7. Criteria likely to be considered by the prosecutor to enter CJIP negotiations

Regardless of who took the initiative to suggest the possibility of a CJIP, the decision to enter into negotiations ultimately rests with the prosecutor who, according to both the Circular and the PNF/AFA Guidelines, shall decide on the basis of whether the company: (i) spontaneously reported the facts at issue; (ii) cooperated in the context of the investigation; and, (iii) already entered into such agreement in the past (which would most likely bar a new CJIP).

Importantly, these three elements are not strict requirements, and do not necessarily prevent prosecutors from entering into CJIP negotiations if they believe, in their discretion, that the circumstances are warranted. As such, it is perhaps not surprising that in the CJIPs concluded so far, (i) the facts were not spontaneously disclosed to the prosecutor and (ii) prior convictions were not taken into account.

Below are some additional points on the above-mentioned criteria.

- **Existence and timing of voluntary disclosure.** The PNF/AFA Guidelines specify that any self-reporting must be made within a reasonable time after the top executives of the company become aware of the offenses. Prosecutors endeavor to verify the impact of such timing on the progress and outcome of the investigations (in particular with a view towards the preservation of evidence and collusion risks). This echoes what is provided in the U.S. Department of Justice Guidelines (9-47.120 – FCPA Corporate Enforcement Policy, November 2017 – last updated in March 2019).

- **Prior convictions**. While the Circular invites prosecutors to consider only the legal entity's prior record, the PNF/AFA Guidelines intend to take into account any sanctions that might have been imposed by a French or foreign court against not only the legal entity but also one of its subsidiaries or even one of its top executives. This also applies when the legal entity has previously been granted a CJIP or a settlement agreement has been entered into with a foreign authority for corruption-related offenses. This clarification seems to go against a cardinal principle under French law whereby punishment attaches only to the specific juridical person which committed the offense.

- **Cooperation**. The need to cooperate with the investigation is indicated in the Circular and further developed in the PNF/AFA Guidelines. In this respect, prosecutors expect companies seeking a CJIP to have actively taken part in revealing the truth by means of an internal investigation or in-depth audit of the offenses and the malfunctioning of the compliance system that allowed such offenses to occur. The cooperation of the company in the criminal investigation is presented as a prerequisite for entering into a CJIP by the PNF, and the PNF/AFA Guidelines indicate that the quality of this cooperation will be a decisive factor for prosecutors in deciding whether to abandon the prosecution proceedings and enter into a CJIP. Furthermore, the PNF/AFA Guidelines specify that the internal investigation should result in a report drawn up and presented to prosecutors describing the offenses with the greatest possible accuracy.

The PNF/AFA Guidelines indicate that the internal investigations carried out by the company must also help in establishing liability of individuals. This requirement is reminiscent of the condition imposed by the DOJ in the 2015 “Yates memo” which required that the identity of the person involved in the corrupt scheme be disclosed by the company that intended to benefit from the cooperation credit (although this condition has since been reduced and now only concerns the identification of all the individuals substantially involved in or responsible for the misconduct at issue). Unlike in the United States, however, French criminal procedure does not allow natural persons to conclude a CJIP; while a settlement mechanism does exist for individuals, companies will have to be cognizant that providing information on individuals responsible for certain conduct may result in those individuals being prosecuted criminally as well.

8. Criteria likely to be considered in the calculation of the public interest fine.

As the French Code of Criminal Procedure offers no further details on how to calculate the public interest fine other than (i) taking into account the benefits derived from the breaches found and (ii) defining a cap of 30% of the average turnover over the last three years, the Circular, the PNF/AFA Guidelines and the CJIPs previously concluded have made it possible to understand in broad terms the methodology applied for calculating the public interest fine. In particular, it appears to be composed of (i) the amount of the ill-gotten gains and, where applicable (ii) an additional penalty aimed at sanctioning more severely the most serious cases.

We note at the outset that the objectives sought by the prosecutors to (i) include the entire amount of the ill-gotten gains and (ii) to adjust the amount of the fine to the seriousness of the misconduct through the additional penalty are not consistent with the legal cap of 30%. Indeed, the higher the amount of the illicit profit, the more likely the offense will be viewed as serious, and the less room there is to apply an additional penalty.

Restitution of ill-gotten gains. The French Code of Criminal Procedure’s provisions indicating that the public interest fine is to be established in proportion to the ill-gotten gains suggest: (i) the amount of the improper advantage is the only reference value to take into account; and (ii) only a portion of such advantage will be included within the public interest fine component. Nonetheless, the precedents to date show that this is not necessarily the case. Indeed, in most of the CJIPs that were concluded as of the time of this Alert (except for that involving Kaefer Wanner – *see infra*), the unlawful profits were completely included in the amount of the public interest fine. Such practice has been endorsed by the PNF in the PNF/AFA Guidelines.

In order to calculate the amount of the improper advantage, both the Circular and the PNF/AFA Guidelines recommend considering both direct and indirect profits gained from the corruption scheme. According to the PNF/AFA Guidelines, the improper advantage will be calculated on the basis of the turnover generated by the corrupt scheme, after deduction of expenses directly attributable to the project. This deduction may only be made from revenue directly related to the corrupt scheme under consideration.

Determination of additional penalty. Depending on the circumstances, the prosecutor is invited to apply aggravating or mitigating factors. Aggravating factors may include (i) the gravity of the corruption scheme, which can result from its public nature and/or its duration, (ii) previous conviction/sanction of the legal entity, (iii) use of resources of the legal entity to conceal corruption-related offenses, (iv) the fact that the legal entity is subject to Sapin II, and (v) the repeated or systemic nature of the corruption-related offenses. According to the Ministry of Justice, the aggravating multiplier must be equal to at least two, in order to result in a situation where the commission of the corrupt conduct ultimately costs the company more than what it benefitted from the scheme. The experience from the CJIPs concluded to date, however, shows that such logic is not applied in practice.

In contrast to the aggravating factors, the Circular and the PNF/AFA Guidelines invite the prosecutor to also consider mitigating factors where they deem that the facts at issue (i) are particularly old, (ii) whenever the

company (a) self-reported them, (b) cooperated during the proceedings, (c) took remedial measures and/or (d) implemented preventive measures. While the Circular and the PNF/AFA Guidelines appear to be consistent in terms of considering aggravating or mitigating factors, there are two points of divergence that should be highlighted. First, the PNF/AFA Guidelines provide that a company's prior convictions may be considered as an aggravating factor, whereas they are only a criteria for assessing the opportunity of settling a CJIP under the terms of the Circular. In addition, as regards the implementation of a compliance program, the Circular states that it will be taken into account by reducing the cost relating to the implementation of a compliance program, rather than by reducing the amount of the fine, which differs from the approach specified in PNF/AFA Guidelines. As described in greater detail below, the seven CJIPs concluded so far offer a good illustration of what enters into consideration regarding the calculation of the public interest fine. They all (except one) included the entire amount of ill-gotten gains and applied an "additional penalty," the amount of which was more or less consequential depending on the aggravating and/or mitigating factors.

International Coordination. The PNF/AFA Guidelines also outline that in the context of multi-jurisdictional negotiations with one company, the determination of the amount of the public interest fine may be discussed with the foreign prosecuting authorities in order to allow an assessment of all the fines and penalties paid by the legal entity.

9. Review of CJIPs entered into to date

Below are summaries of CJIPs that had been concluded as of the time of this Alert.

a. SARL Google France and Google Ireland Limited

On September 3, 2019, SARL Google France and Google Ireland Limited entered into a CJIP with the French financial prosecutor. In its CJIP, SARL Google France and Google Ireland Limited agreed to be jointly liable to pay a 500 million € public interest fine (46,728,709 € charged to SARL Google France and 453,271,291 € charged to Google Ireland Limited). The public interest fine for SARL Google France was calculated based on the theoretical maximum amount incurred (30% of the annual turnover for the last three years) minus the sum of 56,858,528 € that SARL Google France accepted to pay as penalty. The public interest fine of Google Ireland Limited is comprised of the 202,636,215 € as restitution of profits (189,528,428 € of tax evaded and 13,107,787 € for cash flow benefit from the tax evaded sum) and 297,363,785 € as additional penalty. All the estimated ill-gotten profits were included in the fine and increased by the above-mentioned additional penalty. In parallel, the prosecutor applied both mitigating and aggravating factors. With regards to mitigating factors, the CJIP noted the acceptance by SARL Google France to settle its tax debt and the cooperation of SARL Google France and Google Ireland Limited to the criminal investigation. With regards to the aggravating factors, the CJIP noted the magnitude of the amounts of the taxes evaded and the duration of time during which these breaches persisted.

b. Carmignac Gestion SA

On June 20, 2019, Carmignac Gestion (CGSA), the French holding company of the Group Carmignac, entered into a CJIP with the French financial prosecutor in order to resolve an investigation into tax evasion, aggravated tax evasion and concealment and laundering of these offenses. In its CJIP, CGSA agreed to pay a 30 million € public interest fine, comprised of 11,907,719 € as restitution of illegal profits (calculated from the amount of tax evaded from tax authorities and 763,887 € of cash flow benefits from such wrongdoing) and 18,092,281 € as an additional penalty. All the illegal estimated profits were included in the fine and increased by the above-mentioned additional penalty. In parallel, the prosecutor applied both mitigating and aggravating factors. With regards to mitigation factors, the CJIP noted the fact that CGSA accepted to pay a sum of 9,989,740 € as part of a tax levy

procedure. With regards to aggravating factors, the CJIP noted the seriousness of the situation, as characterized by a complex tax arrangement involving several structures, including some voluntarily established in Luxembourg to benefit from an attractive taxation rate.

c. Société Générale SA

On May 24, 2018, French company Société Générale SA entered into a CJIP with the French financial prosecutor. By doing so, it agreed to pay a public interest fine of 250,150,755 € (*i.e.,* 167,437,431 € as a restitution of profits and 82,713,324 € as an additional penalty) and agreed to have its compliance program assessed by the AFA over the course of two years in order to resolve an investigation on active corruption of foreign public agents involving a Libyan intermediary. Société Générale SA was criticized for having financed, through the payment of non-standard commissions, luxury trips and gifts to the benefit of the Libyan Investment Authority's (LIA) executive director in exchange of numerous investments made by LIA to Société Générale SA.

The DOJ started investigating these acts in 2014, and the French financial prosecutor cooperated with the DOJ when it started its own investigation in 2016 by coordinating their investigations and sharing evidence. The U.S. and French authorities eventually decided to split the total amount of the fine (500,301,511 €) in half. The totality of the ill-gotten gains was part of the fine, plus an additional penalty due to the gravity of the facts, the duration of the corrupt behavior and the fact that they involved foreign public officials. The CJIP noted that there was no need to indemnify LIA as part of the CJIP, since 963 million € had already been paid by Société Générale SA within the framework of civil proceedings carried out in front of the High Court of Justice of England and Wales. The Société Générale CJIP is not only the first one to be concluded on the basis of corruption of foreign public officials, but also the first to be concluded in the course of a preliminary investigation. As such, the company did not have to adhere to the legal characterization of the facts, but only to their existence, as opposed to other CJIPs where the signing company had been indicted and thus required to adhere to these two elements.

The CJIP noted that Société Générale SA had improved its compliance and anti-corruption policy and had continued to develop such policies and procedures. The company was given a two-year Monitorship, during which the AFA will assess the quality and effectiveness of its compliance policy and will provide recommendations towards its improvement. The expenses associated with the monitorship shall be paid by the company up to a limit of 3 million €, which is 10 to 15 times greater than the expense cap set out in the three earlier CJIPs with monitors. The CJIP was validated by the court on June 4, 2018.

The Société Générale CJIP is an example of international cooperation, which is also envisaged in the PNF/AFA Guidelines. Such Guidelines indicate that prosecuting authorities of different countries, dealing with the same offenses, are able to coordinate their desired criminal response. In such instances, the determination of the amount of the public interest fine may be discussed between foreign prosecuting authorities in order to allow for a holistic assessment of all the fines and penalties paid by the legal entity.

d. EDF-Related

In 2018, prosecutors entered into three CJIPs involving a corruption scheme within the procurement department of EDF (Électricité de France, a French electric utility company largely owned by the French State). All three companies were involved in active public corruption for having yielded to the requests of EDF's procurement officer in order to obtain and maintain maintenance contracts. The prosecutor took into account, as aggravating factors, the duration of the misconduct and the fact that the offense had been made within the framework of a contractual relationship with an operator responsible for a public service mission. Although the amount of the public interest fine varied for each case, depending on the gravity of the misconduct and the amount of the profits illegally obtained from the misconduct, the damages awarded to EDF was invariably 30,000 € for each of the

defendants. These CJIPs concluded with the Nanterre prosecutor, confirming that corruption-related prosecutions do not fall within the exclusive competence of the French National Prosecutor.

- *SAS SET Environnement*: On February 14, 2018, the French company SAS SET Environnement entered into a CJIP with the Nanterre prosecutor, agreeing to pay a public interest fine of 800,000 € (680,000 € as a restitution of profits and 120,000 € as an additional penalty, to be paid in four installments) and 30,000 € in damages. In addition, SAS SET Environnement committed to implementing and complying with an effective compliance program under the supervision of the AFA for two years (with such supervision-related costs capped at 200,000 €). SAS SET Environnement is a small company, with 125 employees and turnover of between 10 and 20 million € over the past eight years. This case is an example of how companies which do not meet the thresholds provided by Article 17 of Sapin II (companies with at least 500 employees and a turnover of over 100 million €, or companies that are part of a group with a total of at least 500 employees and a consolidated turnover above 100 million €) may nonetheless be compelled to implement a compliance program in line with the legal requirements of Article 17. Here again, the entire amount of the profit illegally gained was included in the public interest fine. In order to assess the amount of the additional penalty, the judge took into account certain aggravating factors and also highlighted, as mitigating factors, the fact that: (i) the President of the company involved in the offense left the company and sold his shares; (ii) the General Secretary and the Chief Financial Officer involved in the offense were terminated; and, (iii) new shareholders and a new management team not involved in the offense are now in place. The CJIP was approved by the court on February 23, 2018.

- *SAS Kaefer Wanner*: On February 15, 2018, the French company SAS Kaefer Wanner (a subsidiary of the German group Kaefer) entered into a CJIP with the Nanterre prosecutor, agreeing to pay a public interest fine of 2,710,000 € (in twelve installments) and 30,000 € in damages. They additionally agreed to submit to the AFA's control for 18 months in order that the AFA can assess the company's then-current compliance program and make recommendations (with such supervision-related costs capped at 290,000 €). It is interesting to note that the French authority will be monitoring the French subsidiary of a foreign entity, which may result in French-imposed compliance program requirements spreading beyond French borders. In order to assess the fine, the above-mentioned aggravating factors were taken into account, however the prosecutor also noted a number of mitigating factors, including the fact that the company cooperated with the investigation and took measures to detect and prevent corruption. The CJIP highlighted that SAS Kaefer Wanner changed its management and governance rules, provided anti-corruption training to its employees and strengthened its ethics program. All these measures resulted in a fine which was lower than the amount of the ill-gotten gains (the illegal profits were estimated to 3.3 million € whereas the fine was set to 2.71 million €). This is the only case so far where the mitigating factors weighted more than the aggravating ones in the assessment of the fine. The court's decision approving this CJIP has not been published on the AFA's website.

- *SAS Poujaud*: On May 4, 2018, the French company SAS Poujaud (subsidiary of the French group Altrad) entered into a CJIP with the prosecutor, agreeing to pay a public interest fine of 420,000 € (240,000 € as a restitution of profits and 180,000 € as an additional penalty, to be paid in two installments) and 30,000 € in damages. The company was additionally required to submit to a compliance program under AFA's supervision during two years (with such supervision-related costs capped at 276,000 €). All the ill-gotten profits were included in the fine and increased by the above-mentioned aggravating factors. With regards to the mitigating factors, the prosecutor noted that the

fact that SAS Poujaud did not spontaneously reveal the facts, and did not cooperate during the proceedings, deprived the company of benefitting from mitigating factors. Although SAS Poujaud did not benefit from mitigation based on these elements, these factors were not used to aggravate the assessment of the faulty behavior by the prosecutor and to increase the amount of the fine. The CJIP nevertheless noted two mitigating factors: (i) the implementation of an Ethics Code; and (ii) the fact that certain directors left the company. The CJIP was approved by the court on May 25, 2018.

e. HSBC Private Bank (Suisse) SA:

On October 30, 2017, the Swiss bank HSBC PRBA entered into a CJIP with the prosecutor and, as such, gave rise to the first-ever CJIP. In its CJIP, HSBC agreed to pay a 157,975,422 € public interest fine (86,400,000 € as a restitution of profits and 71,575,422 € as a penalty) and 142,024,578 € in damages, in order to resolve a four-year criminal investigation into the bank's assistance in helping French clients conceal their assets from the French tax administration.

HSBC was indicted for: (i) unlawful banking and financial solicitation of prospective French clients committed by unauthorized persons; and (ii) laundering the proceeds of tax evasion, with the latter offense being explicitly eligible for the CJIP and the former offense being considered as "connected" to the latter offense.

The entire amount of the ill-gotten gains was included in the public interest fine, and additional financial penalties were also imposed based on the seriousness of the facts and the duration of the misconduct. The settlement refers to the fact that the bank "neither voluntarily disclosed the facts to the French criminal authorities, nor acknowledged its criminal liability during the course of the investigation" and "only offered minimal cooperation in the investigation." However, the HSBC CJIP also noted that from the time the investigation was launched until December 2016 (when Sapin II came into force), the French legal system did not provide for a legal mechanism that encouraged full cooperation. While it is also the case for the other CJIPs, the HSBC CJIP is the only one to contain such a statement. At the time of the HSBC CJIP, the Circular had not been issued. Since then, the above-mentioned Circular has confirmed that self-disclosure is to be taken into account as a criteria to offer the company at fault the opportunity to conclude a CJIP and as a mitigating factor in the calculation of the public interest fine. Here, and as opposed to the other CJIPs concluded to date, the total amount of the fine corresponds to the maximum public interest fine allowed under Sapin II (30% of the company's average gross annual turnover over the last three years).

The fact that the CJIP did not require HSBC to implement an effective compliance program under the supervision of the AFA likely results from the fact that this CJIP was concluded for offenses related to the laundering of tax evasion profits, activities which neither fall within the primary competence of the AFA nor are the primary focus of Sapin II-required compliance programs. Following the court's approval of the CJIP on November 14, 2017, the criminal prosecution against HSBC was formally terminated on November 28, 2017 when the bank complied with the requirement to pay 300 million € within a ten-day period. This illustrates one notable difference between the CJIP and the DPA in the United States. Whereas DPAs in the United States systematically defer prosecutions for a certain period of time pending satisfactory conclusion of whatever terms the DPA sets forth, proceedings in France against a company entering into a CJIP are formally terminated on the date of which its obligations are met, irrespective of the potential immediateness of such obligations.

D. Creation of an Affirmative Obligation to Implement a Compliance Program

1. Scope

Under Sapin II, certain companies are required to implement a compliance program in order to prevent and detect acts of corruption. The compliance program requirement applies to: (i) companies established under French law with at least 500 employees and with a turnover of over 100 million €; and (ii) companies established under French law that are part of a *group* with a total of at least 500 employees, where the parent company is headquartered in France, and the group has a consolidated turnover above 100 million €. These obligations also apply to state-owned companies and to the subsidiaries of entities subject to Sapin II.

If a company/legal entity meets these criteria, the requirement to implement an adequate compliance program also applies to its president, chief executives (directeurs généraux), managing directors (gérants) and, under certain circumstances, members of the management board. The French legislature intentionally made the compliance program broadly applicable and placed responsibility on natural persons in an effort to ensure that anti-corruption compliance programs would be implemented throughout French companies subject to the law.

2. Entities' Compliance Programs

Companies and legal entities falling under the scope of Sapin II are required to implement anti-corruption compliance programs that include the following eight elements:

- a code of conduct defining and illustrating the prohibited conducts likely to constitute an act of corruption or influence peddling ("Code of Conduct");
- a regularly updated assessment of the potential risks of exposure to external corruption ("Risk Assessment" or Cartographie des risques);
- internal whistleblowing procedures designed to report violations of the Code of Conduct;
- third-party due diligence and risk-assessment procedures for clients, lead suppliers and intermediaries;
- internal or external financial controls ensuring that the company's books and records are not used to conceal acts of corruption or influence peddling;
- training programs for executives and employees potentially exposed to corruption risks;
- disciplinary procedures in the event of corruption, influence peddling and related misconduct by employees; and
- internal mechanisms to evaluate and monitor the effectiveness of the compliance measures.

E. Creation of a New Anti-Corruption Agency: AFA

As noted above, Sapin II created the AFA, the authority primarily responsible for assisting companies and entities in preventing and detecting acts of corruption and influence peddling in both the public and private sectors. The AFA has policy-making authority and enforcement powers limited to administrative sanctions, although it may refer cases to the prosecutor for criminal action if the AFA uncovers possible criminal activity while performing its

mission. Its head is appointed by the President of France for a non-renewable six year term, and reports to both the Ministers in charge of Justice and the Budget (Ministre de la Justice and Ministre du Budget). The first and current head of the AFA is Charles Duchaine, a former prosecutor, who was appointed in March 2017. The AFA is notably composed of two sections: (i) the Advisory Division, in charge of helping the competent private and public actors to prevent and detect corruption act, by elaborating recommendations and providing support to public and economic actors and (ii) the Control Division, in charge of controlling the quality and the efficiency of the procedures implemented pursuant Sapin II and controlling the execution of requirements flowing from prosecutions or CJIP settlements.

1. Advisory Mission

On October 2, 2018, the AFA released its Business Support Charter (Charte d'appui aux entreprises), which establishes the framework for the relationship between companies and the AFA's Advisory Division for the purposes of its mission to help organizations prevent and detect corruption and influence peddling. Since the needs of companies may differ according to their size, sector of activity, economic model, and the sophistication of their compliance system, the AFA has set forth three categories of support.

The first category of support is referred to as generic support, which is intended for all companies concerned with detecting and preventing corruption, regardless of the company's size or sector. Generic support consists of the AFA developing, updating and disseminating the French anti-corruption framework, on the basis of Sapin II's legal requirements. This includes the AFA Recommendations (*see* below), practical guides, responses to general interest questions published on the AFA website, and all other relevant standards for preventing and detecting corruption.

The second category of support is referred to as specific support. It consists of the AFA clarifying or providing expertise on issues raised by a group of companies that have already set up an anticorruption program or are in the process of doing so. The AFA can provide specific support through proofreading documents for the companies or through technical workshops for small groups, which will be organized by sector of activity, job (i.e., compliance officer), or anticorruption issues.

The third category of support provided by the AFA is individual support, which consists of the AFA responding to the specific questions of a specific company. This can be done by mail or email, or through individual coaching at the request of the company for a period not to exceed five months. In the case of individual coaching, the AFA will guide a company in relation to the implementation or updating of its compliance program, in an effort to ensure that the company understands the applicable anticorruption standards as well as the methods available for deploying a compliance program. AFA's guidance will be based on documents produced by the company and will be discussed during regular meetings between the company and the AFA scheduled jointly by the parties. It does not, however, constitute a certification of the company's compliance program. All companies, regardless of size and sector, can request individual coaching by the AFA, although AFA will evaluate the request and determine whether individual coaching or another form of support would be more appropriate for the particular request. The individual coaching will last as long as agreed between the AFA and the relevant organization (not to exceed five months) unless the organization decides to end the mission before the agreed date or the AFA considers that the company does not respect its commitment to allocate relevant resources to the relevant project. Companies are not obligated to follow the recommendations made by the AFA in the course of the coaching period, and the information shared with the relevant AFA agents is confidential and subject to professional privilege. It is important to note that the support and advisory mission of the AFA is separate from its enforcement / control mission, as each function is exercised by a different division of the AFA.

a. AFA's Recommendations on the Compliance Program

On December 21, 2017, the AFA issued specific recommendations concerning some of the required elements of a compliance program under Sapin II, the relevant parts of which are included below:

- **Top Management's Commitment to Preventing and Detecting Corruption**: While not formally part of the Sapin II legal requirements, the AFA emphasizes in its guidelines that senior management's commitment to a zero-tolerance policy is fundamental for preventing and detecting corruption.

- **Anti-Corruption Code of Conduct**: In addition to the legal requirements set forth in Sapin II, the AFA recommends inter alia that the Code of Conduct: (i) be initiated by the organization's top management; (ii) set out the organization's values and commitments; (iii) describe the internal whistleblowing system offered to employees; (iv) be written in French and translated to be understood by foreign employees; (v) be used as a tool for external communication when dealing with customers, users, suppliers and any other partners of the organizations; and (vi) be regularly updated, especially after any significant update of the risk map (e.g., in the case of a reorganization or restructuring).

- **Internal Whistleblower System**: While Sapin II requires companies to implement an internal whistleblower system allowing employees to disclose conduct or situations that do not comply with the company's Code of Conduct, the AFA made some recommendations in line with the requirements pertaining to the whistleblower procedure as a more general feature of a company's organization, set out by Article 6 and seq. of the Sapin II (*see* below). As such, the AFA encourages entities to implement a single whistleblowing system and recommends that it specify the information required with respect to the Article 6 whistleblowing system, including the following: (i) the person in charge of receiving whistleblowers' reports; (ii) the measures taken to ensure confidentiality of the disclosures and the identity of the persons alerting the company and affected by the alert; (iii) the procedures for communicating with the whistleblower to inform him/her, respectively, of the progress made with processing and handling the alert; and (iv) where appropriate, the policy on processing anonymous reports. The whistleblower protection status may be applied in the framework of this system if conditions discussed in greater detail below are met.

- **Risk Mapping**: According to the AFA, the risk mapping must be comprehensive, formalized, and adaptable over time to changing risks. The AFA's guidelines provide a specific methodology that they recommend companies follow consisting of: (i) identifying risks that are inherent in the organization's activities; (ii) assessing the company's exposure to "gross risk" of corruption through the analysis of risk factors or sources (such as high-risk countries, new products, complex contracts, business pressure); (iii) determining the probability of occurrence of the identified risks (for instance, based on a history of incidents); (iv) assessing the existence of aggravating factors (by applying risk coefficients); (v) assessing the adequacy and effectiveness of mitigating measures in order to determine to what extent they allow computation of the "net" or "residual" risks exposure; (vi) prioritizing risks depending on their scores, and (vii) implementing an action plan.

- **Third-Party Due Diligence Procedures**: While Sapin II requires companies to conduct due diligence on certain categories of third parties (customers, lead suppliers and intermediaries), the AFA considers that such categories are only "priorities" and recommends that companies review (based on risk) all the third parties with which they have or are about to start a relationship. The AFA's guidelines provide that due diligence should be conducted before starting any relationship, updated periodically, and proportionate to the risk level. Among the information that the companies are recommended to assess are sanctions lists. In addition to conducting third-party due diligence, the AFA recommends heightening third parties' awareness

by: (i) notifying them of the company's compliance program; (ii) providing them with the company's Code of Conduct and anti-corruption training; and (iii) requiring them to provide a written commitment to combat corruption (including through anti-corruption clauses that are incorporated into risky contracts) and to check the integrity of their subcontractors.

- **Accounting Control Procedures**: In its guidelines, the AFA states that accounting control procedures have two main goals; first, safeguarding the company's assets and resources by checking that operations are well-managed and allocated resources are properly used; and second, ensuring that the company's books and accounts are not used to conceal acts of corruption. Such procedures provide reasonable assurances that a company provides a reliable, regular, sincere, faithful, and complete picture of its accounting and financial situation. Accounting controls can include controls (internal procedures), audits (independent assessments), or both, and can be carried out internally or externally. In any case, the AFA recommends three levels of controls.

- **Corruption Risk Training**: Companies are required to implement "robust [and] appropriately designed" internal anti-corruption training. Such training should particularly be attended by board members, directors, managers, and employees that are most exposed to corruption risks. Over time, all employees should have been trained to prevent and detect corruption. The training may be delivered internally, by the company itself, or through external consultants, and the company should develop a set of indicators to track the implementation of the training program. While Sapin II only refers to managers and the most exposed employees, the AFA recommends that other employees also be trained, at least on a general basis.

- **Internal Monitoring and Assessment System**: In addition to what is required by Sapin II, the AFA recommends three levels of controls to evaluate the company's compliance program. The first level of controls, performed by operational or support staff, or by line managers, aims to ensure that the all operational or support tasks are carried out in compliance with the company's procedures. The second level of controls, performed by the head of compliance (or other designated manager), is meant to ensure that the first level of controls is properly implemented and that the internal monitoring and assessment system is working properly. The third level of controls, which typically consists of "internal audits," is intended to ensure that the system to prevent and detect corruption complies with the company's requirements and is efficiently implemented and kept up to date. Based on the risk mapping, the company is to develop an audit plan identifying all functions and individuals involved in the monitoring system.

While companies already subject to the U.S. FCPA or the U.K. Bribery Act are likely to have already implemented compliance programs that are largely compliant with the above-mentioned Sapin II requirements, there are certain specificities that need to be considered, including the need to follow applicable rules under French Labor Law and Data Privacy Laws. We note that, although the AFA's guidelines are not legally binding, in practice, the AFA generally follows its own recommendations—which in many instances are broader than what the law requires—when conducting controls to assess companies' compliance programs.

b. AFA Guides on specific themes

As part of its advisory mission, the AFA also publishes guidelines and handbooks on particular topics. Since its creation, the AFA has published guidance on numerous subjects, including on key components of the compliance program such as third parties due diligence, risk mappings, and codes of conduct, and on themes such as conflicts of interest and facilitating payments. The AFA also published handbooks on monitorships, as well as sanctions issued by the AFA Sanctions Committee, and as of the time of this Alert, guides on gifts and entertainment, as well as anticorruption due diligence in the framework of mergers and acquisitions were being prepared.

On February 2019, the AFA published its Guide on the anticorruption compliance function in companies. In the guide, the AFA underlines the strategic stake and cross-functionality of the anticorruption compliance function and emphasizes the role of the governing body with regards to the effective governance of the anticorruption compliance program within the organization. The AFA points out that there is no “one-size fits-all” anticorruption compliance program and the governance of the compliance function must be tailored by the specificities of particular companies.

- **Anticorruption compliance function.** The Guide on the anticorruption compliance function defines the anticorruption compliance function as a strategic transversal element under the responsibility of the governing body. The Guide on the anticorruption compliance function indicates that although the main function of the Chief Compliance Officer is to implement and deploy the anticorruption program within the company, its role may be quite broad. The AFA details 11 eleven tasks that, in its view, may be assigned to the compliance function, including monitoring; controlling and reporting on the implementation of the program, and coordinating all stages of an internal investigations following evidence or allegations of potential misconduct. The involvement of the Chief Compliance Officer, according the Guide, may also extend beyond anti-corruption, to include topics such as ethics, anti-money laundering, sanctions, data protection, or antitrust. According to the AFA, in this context, it would recommend establishing matrices showing all the roles and responsibilities of all the functions intervening in all the different compliance sectors.

- **Governance of the anticorruption compliance function**. As stated above, the governance of a company’s compliance function will be determined by the characteristics of the organization. Accordingly, the compliance function can either be integrated into another service line (such as legal or finance) or it may be a dedicated function. The compliance function must be clearly identified within the organization, as a driver of the elaboration and implementation of the compliance program and must have sufficient financial, human and material means allocated to this end. The Chief Compliance Officer shall be formally designated by the governing body. The AFA Guide on the anticorruption compliance function suggests that its appointment should be communicated to all employees by an internal memo of the governing body. In addition, for governance purposes, it is recommended to have an integrated and independent compliance function within the organization that would report only to the governing body. Thus, as for the role of the Chief Compliance Officer, the Guide on the anticorruption compliance explains that he or she also needs to be involved in the implementation of strategic projects and in the structuring of key decisions, including mergers and acquisition, new products, accessing new markets or investment in new countries.

- **Qualifications and Mandate of the Chief Compliance Officer**. When nominating the Chief Compliance Officer, the governing body shall choose someone that has sufficient integrity, knowledge of the organization and strong regulatory skills. The Chief Compliance Officer is in charge of coordinating the risk mapping, the code of conduct, the training program, the escalating procedure, the disciplinary regime, the third parties due diligence process, and (in coordination with finance personnel) the accounting procedures and the internal controls.

- **Liability of the Chief Compliance Officer.** The AFA Guide on the anticorruption compliance function addresses the issue of potential criminal liability of the Chief Compliance Officer. It indicates that in the event of cases of alleged corrupt activities, Chief Compliance Officers will not be held liable unless they participated in the conduct or failed to prevent it in a manner that was inconsistent with the performance of their professional duties. The AFA Guide thus reiterates that the governance body of the company is the unit ultimately responsible for the implementation of the anticorruption program.

2. Control Mission

a. Process

The AFA can initiate controls to assess an entity's compliance with the Sapin II compliance obligations on its own or at the request of, inter alia, either the President of the French High Authority for the Transparency of Public Life (Haute autorité pour la transparence de la vie publique) or the French Prime Minister.

As partly presented in the "Charter of Rights and Duties of Parties under Control" issued by the AFA in October 2017 and experienced in real controls, the process can be divided into the following eight steps:

- **Control Notice**. The AFA sends a control notice to the representative of the company subject to the control by way of an official letter. This notice both informs the company of the identity of the agents in charge of the control, and requires the company to answer a general questionnaire of 163 questions focused on the compliance program and the company's activities and organization. After the first wave of controls, this questionnaire (in slightly revised form) was made available on the AFA's website.

- **Communication of Documents and Response to the AFA Questionnaire**. The company subject to the control has 15 days to submit its answers to the aforementioned questionnaire and communicate supporting documents as well as those requested by the AFA through the questionnaire. Since the questionnaire has been made available, many French companies have wisely begun to start gathering information on a proactive basis in order to be able to provide required responses easily and without freezing the organization in case of a control. It is worth noting that the Sanctions Commission indicated in its decision dated July 4, 2019 (*see* below) that the AFA is entitled to request documents that were established before the entry into force of Sapin II's Article 17.

- **Discussions with the AFA**. A preliminary courtesy meeting may be organized between the AFA's agents and the company subject to the control.

- **Document Review ("contrôle sur pièce")**. The AFA undertakes its review of the documentation provided, which usually gives rise to follow-up questions from the AFA to the company subject to the control. In certain controls, such questions have taken the form of a new questionnaire.

- **Onsite Control Notice**. Fifteen days before the onsite control, a notice is sent to inform the company subject to the control of the dates on which the agents will come onsite and the identity of individuals that the control team will interview. They interviewees regularly (if not systematically) can include external stakeholders (such as customers). In 2017, the average number of interviews conducted by the AFA in this context was 21, although in certain controls the number of interviews can be significantly higher.

- **Onsite Control**. The AFA reviews documentation and conducts interviews in the premises of the company subject to the control. As explained below, the Sanctions Commission held that the absence of record of minutes during the interviews does not void the procedure.

- **Additional Discussions and Exchanges**. The company subject to the control may have further exchanges with the AFA after the onsite control ends, although new documents communicated after such deadline are not to be taken into account by the AFA.

- **Control Report**. The AFA eventually prepares a report discussing the control process and assessing the quality of the anti-corruption program in place within the entity, with a specific emphasis on “tone at the top.” The report is divided into “Observations,” “Recommendations,” and “Findings of Breach.”

- **Observations of the Company Subject to the Control on the Control Report.** The company subject to the control has two months to comment on the AFA’s findings and to challenge, as the case may be, their merits.

- **Issue of the Final Report.** The AFA issues the report in its final version, replying, as the case may be, on the company’s comments and arguments.

Concluding the control, the AFA will have a number of choices. Its President may issue a warning and request that corrective action be taken. Alternatively, it may decide to initiate enforcement proceedings before the AFA’s Sanctions Commission. If an enforcement proceeding is held, the company will have the opportunity to present observations at a hearing. The Sanctions Commission may impose fines on individuals of up to 200,000 € and a fine of up to 1 million € on companies. The Sanctions Commission can also enjoin the company to take appropriate action to adopt an effective compliance program (or elements of an effective compliance program) within a certain period of time (the maximum of which is three years). These sanctions can be cumulative, but the amount of the fines shall be proportionate to the severity of the infringement and will take into consideration the financial situation of the person or company in breach. Any decision issued by the AFA’s Sanctions Commission ordering an injunction or a financial penalty may be made public and can be appealed before administrative courts. On this matter, the AFA’s Control Division has indicated that appeals against the decisions of the Sanctions Commission are in the first instance the responsibility of the Paris Administrative Court.

Since the AFA is responsible for reviewing compliance with the obligations to prevent and detect corruption and influence peddling described above, it does not have to establish the elements of underlying criminal offenses of corruption and influence peddling in order to sanction companies or bring them before the Sanctions Commission. In other words, a company can be sanctioned for not having in place the elements of a compliance program required by Sapin II, whether or not an act of underlying act of corruption can be established.

b. Statistics

The AFA’s activities to date have shown it to be effective and ambitious in fulfilling its mission. The AFA contemplates implementing control measures in approximately fifty private sector entities per year (out of the 1,570 private sector entities subject to the AFA’s controls at the time of this Alert) to ensure compliance with Sapin II’s requirements. However, and as stated above, the first controls, which began in October 2017 involving six companies, as well as the following ones launched in 2018, show that not only does the AFA asses compliance with the legal requirements as set out in Article 17 of Sapin II, it also assesses companies’ compliance with its own recommendations—which, as explained above, appear broader than what is stated in the letter of the law. Since its creation, the AFA launched 53 controls, out of which 32 have been on economic actors and 15 public actors. Of the 47 controls launched in 2018, 43 of them were carried out at the initiative of the AFA and 4 were carried out following the execution of a CJIP.

c. Lessons learned from the AFA’s controls

So far, nearly all controlled companies have been cited for some form of breach. Based on the first control reports, the following points and expectations of the AFA appear worthy of focus:

- **Tone at the top**: the AFA has only made recommendations in this respect, as this is not, *per se*, part of the requirements of Article 17. However, the controls highlighted the key role of a company's managers (broadly defined), who need to be genuinely included and pro-active in the implementation of compliance programs as well as in the communication of the "zero tolerance" policy within a company. It is noteworthy that these requirements are similar to what is expected by U.S. authorities when evaluating compliance programs. The AFA also recalled that the compliance function within a company needs to be sufficiently resourced and able to act independently in order to achieve its mission.

- **Risk Assessment:** the AFA has focused extensively on the existence of a corruption Risk Assessment and the methodology applied by the company. The Risk Assessment needs to be comprehensive and cover all potential corruption risks that the organization can face. The AFA has carefully checked that all the steps involved in the assessment, from identification of such risks to implementation of remedial actions, are documented. These risks must be assessed based on a variety of criteria, including financial, geographical, commercial or political aspects of the company's activities. Some of these criteria have been identified as involving higher risks by the AFA (i.e., public tenders, exports, and relations with institutional entities located abroad). It is noteworthy that this recommended comprehensive evaluation by the AFA appears to go beyond other international guidance on conducting risk mappings, which counsel towards implementing a risk-based approach.

- **Code of Conduct:** the AFA specified that the definitions of the different types of corrupt behavior and influence peddling should be clear and complete, and the illustration of such conduct should reflect the findings contained in the Risk Assessment. Furthermore, in May 2019, the AFA published pedagogical support materials providing clear definitions of the various criminal offences related to corruption. Finally, the AFA has also specifically focused on the internal (*i.e.* available on the company's intranet) and external (*i.e.* provided during the hiring process) communication of the Code of Conduct.

- **Third-party due diligence:** third-party due diligence has been another key area of focus for the AFA, which insisted on the involvement of the compliance function and its participation in decision-making at the on-boarding stage and during periodic recertification of these relationships. These controls have also been the occasion for the AFA to clarify that all third parties needed to be assessed and not only the "*client, first ranked vendors and intermediaries*" as specified in the Sapin II. It will therefore be important for companies (particularly large multi-national companies with thousands of vendor and/or supplier relationships) to develop a risk-based approach to assessing their third party relationships in a manner that will satisfy the AFA's expectations.

- **Training programs:** in some reports, the AFA specified that anti-corruption training should be provided to all employees. The AFA also insisted on the fact that such training needed to cover influence peddling in addition to anti-corruption offences.

- **Financial controls**: the AFA has stated that all financial and accounting controls should be documented and consistent with the findings contained in the Risk Assessment. The AFA has also indicated that such controls may consist of both first and second-level controls.

- **Whistleblowing system:** among other features, the AFA specified that companies could implement a single whistleblowing system designed to report any violations of the Code of Conduct, as well as any other criminal offences as required by Articles 6 to 16 of the Sapin II.

- **Disciplinary procedures:** the AFA insisted that examples of disciplinary measures applied following violations of the Code of Conduct should be communicated to employees.

- **Evaluation and monitoring of the compliance program:** finally, the AFA determined that internal mechanisms to assess and monitor the effectiveness of compliance measures needed to integrate action plans reflecting the issues identified at each level of control. Sufficient resources also need to be allocated to the third level of control to enable them to control the company's compliance with the new anti-corruption regulations.

d. AFA's Sanctions Commission Activity

On July 4, 2019, the Sanctions Commission of the AFA issued its first (and so far only) decision. The case brought before the Sanctions Commission relates to failures allegedly committed by a company (subsequently publicly identified as Sonepar) in implementing its anti-corruption compliance program. According to the AFA, following a control that was undertaken between October and December 2018, the company had failed to implement the following elements of an effective compliance program: (i) an anti-corruption risk-mapping, (ii) a Code of Conduct, (iii) third-party due diligence procedures, (iv) accounting control procedures and (v) an internal control and evaluation system. The AFA requested the Sanctions Commission to impose (i) an injunction on the company and its president to align its compliance program with the requirements set out by Sapin II before the end of 2019; and (ii) in the event of violation of the such injunction, a fine of 1 million € on the legal entity and 200,000 € on the president of the company. Sonepar, on its end, raised several procedural arguments and argued that the substance of its compliance program as of the day of the Sanctions Commission hearing was effective.

On the procedural aspects, it transpires from the decision that (i) although information and documents that relate to a period prior to the entry into force of Sapin II cannot be used as a grievance for a failure to comply, they may nonetheless be requested if they are relevant to the AFA control; (ii) the fact that no minutes are recorded from the AFA interviews is not a ground for nullity on the basis of a violation of the contradictory principle; (iii) the presence of the AFA Director at the hearing was not a ground for dismissal, as he was not present during the deliberations and (iv) the status of the anticorruption compliance program is assessed *at the day of the Sanctions Commission hearing* and not at the time when the AFA finishes its control.

On the merits, the decision noted that (i) with respect to the risk-mapping, there is no obligation to follow the methodology prescribed by the AFA in its recommendations, meaning that there is no one single method for companies to follow in performing this exercise, as long as it is sufficiently robust and conducted in good faith; and (ii) the illustrations of prescribed behaviors to prohibit corruption that are to be incorporated in the Code of Conduct can instead be incorporated in a more general referential of documents including a compliance guide.

On the whole, the decision was seen (and described) as a victory for Sonepar, who was not sanctioned financially and who was considered, as of the time of the Sanctions Commission hearing, to have implemented a compliance program consistent with the required elements of Sapin II. The decision thus contains some important lessons for companies that may find themselves subject to an AFA control, and who may have some deficiencies in their compliance programs at the time of such a control. As a result of the fact that a breach will be assess as of the time of the Sanctions Commission hearing (and not at the time of the control), it will be important for companies to continue to improve and adapt their programs (particularly based on any AFA recommendations) to avoid the likelihood of sanction if they are brought before the Sanctions Commission.

3. Oversight of compliance with law 68-678 (the "French Blocking Statute")

Another feature under Sapin II is that the AFA may verify, at the request of the Prime Minister, compliance with the French "Blocking Statute" where a company headquartered in France is subject to a monitorship arising out of settlement with a foreign authority and has to transfer information to the foreign authority in that context. Sapin II

does not, however, mention that the AFA would carry out similar reviews for Blocking Statute compliance when the foreign settlements involve offenses outside of corruption or influence peddling. The law similarly does not indicate that the AFA should play this role in the context of foreign-led *investigations* (as opposed to completed settlements / monitorships). However, the PNF/AFA Guidelines may expand the powers of the AFA in this regard as they state that:

> when a company suspects or detects an offense of transnational corruption within its own organization in the course of performing a resolution imposed on it by a foreign authority, it must inform the AFA of this offense before communicating this information to the foreign authority. The AFA shall assess if such a communication might be a violation of [the French Blocking Statute]. The AFA informs the [prosecution] of the progress of the disclosure to the foreign authority to allow the [prosecution] to assess if the offenses detected fall within its field of competence.

In other words, although the stance adopted in the PNF/AFA Guidelines may be intended to ensure that a legal entity is in compliance with the French Blocking Statute, it also seemingly places the legal entity in a position where it would be obligated to report to the AFA information relating to the commission of an offense, placing it in a delicate situation with respect to its right against self-incrimination.

4. Interactions between the AFA and French prosecutors

The AFA does not itself have the authority to investigate bribery, nor does it have authority to impose criminal penalties, both of which continue to be the purview of prosecutors (including the PNF). Although Sapin II has been adopted relatively recently, it has already prompted increased cooperation and coordination between the AFA and prosecutors.

Interactions in the context of the negotiation of the CJIP. The implementation of the monitoring program following a CJIP is one area of collaboration between the AFA and prosecutors. The PNF/AFA Guidelines outline that when assessing (i) the measures and procedures and (ii) the cost of the program to be included in the agreement, the PNF shall consult with the AFA.

Interactions in the context of the implementation of the CJIP. The AFA is required to advise the PNF of any difficulty encountered in the payment of the provision for covering the expert monitoring fees.

Interactions in the context of the implementation of a foreign monitorship. As noted above, the PNF/AFA Guidelines specify that when a company suspects or detects the commission of offenses of transnational corruption within itself in the course of performing a transaction imposed on it by a foreign authority, it must inform the AFA which, in turn shall inform the prosecutor of the progress of the disclosure procedure to the foreign authority to allow the former to assess whether the offenses detected fall within its competence.

Interactions in the context of an AFA control. In accordance with both Article 40 of the French Code of Criminal Procedure and Article 2 of Sapin II, AFA agents shall report to the prosecutor any information they become aware of in the context of their mission when such information is likely to prove the commission of an offense. In 2018, the AFA issued five reports to prosecutors pursuant to Article 40 of the French Code of Criminal Procedure. One example is reported to be a reporting by the AFA to the prosecutor of information concerning the French company Sonepar following the AFA control of that company. The AFA is reported to have transmitted to the prosecutor information and documents collected during the control that were potentially relevant to antitrust and tax evasion breaches.

F. Creation of a Court-Imposed Monitorship

Another novelty of Sapin II is that judges may resort to a new penalty in corruption and influence peddling cases. Courts can sentence companies found guilty of corruption or influence peddling to a form of remediation by requiring them to submit to a compliance program under the supervision of the AFA for a maximum duration of five years. The requirement to submit to a monitorship may also be included as part of the CJIP settlement described above for a maximum duration of three years. A monitorship has been included in all of the corruption-related CJIPs so far, with durations of between 18 months and two years. In both instances, the AFA reports to the prosecutor at least annually on the implementation of the program. The AFA will also be able to rely on the help of "experts" or "qualified authorities," suggesting that the arrangement may eventually bear some similarities to corporate monitorships as used in the U.S. and other jurisdictions to assist regulators in determining whether a corporate defendant is meeting its obligations deriving from a settlement agreement or court order. Nonetheless, to be similar to monitors used by U.S. authorities, such experts would have to be chosen by the company and approved by the prosecution authorities, which is not currently envisioned under the Sapin II framework. Nonetheless, any cost incurred by the supervision of the AFA and the assistance of such experts are to be assumed by the company, although such costs shall not exceed the amount of the fine incurred for the offense of which the subject was prosecuted.

As partly presented in the "Guidelines on the court-imposed monitorship" issued by the AFA in April 2019, the process can be broken down into the following five steps: (1) the initial control by the AFA; (2) definition of an action plan by the company; (3) AFA validation of the action plan; (4) implementation of the action plan and permanent interactions between the AFA and the company over a longer period of time, and (5) the final control report sent to the prosecutor by the AFA.

The PNF/AFA Guidelines clarified in some respects the length of an AFA monitorship under a CJIP. In addition to what is legally provided for as far as a maximum duration (three years pursuant to Article 41-1-2, I, 2° of the French Code of Criminal Procedure), the PNF/AFA Guidelines provide for a minimum of two years. In most CJIP settlements to date, this two year period has been followed (with the exception of the Kaefer Wanner CJIP, which was for 18 months), which seems to reflect a view that, in the view of PNF and AFA, this is the minimum period that will allow the AFA to perform an adequate review of a company's compliance program. In addition, the PNF/AFA Guidelines indicate that, if a compliance program obligation is considered in the context of a multi-jurisdictional negotiation, it is preferable to appoint only one monitor. Should the company at issue have its registered office or operating base in France or carry on all or part of its economic activities on the French territory, the PNF/AFA Guidelines suggest (without pointing to a specific legal basis for doing so) that the AFA shall be appointed monitor in this instance. In cases involving other jurisdictions and regulators, it will be interesting to see how monitors are appointed to satisfy this expectation.

G. Reinforced Protection for Whistleblowers

1. Background

Despite a historically strong cultural preference against denunciation, French law has introduced incremental protections and rules for whistleblowers. While the protection system progressively introduced by law was disseminated throughout various statutes and limited to whistleblowers reporting specific wrongdoings (corruption, public health, conflict of interests, offenses and clear and serious breaches of law), Sapin II includes a harmonized and strengthened whistleblower protection regime. This protection regime has recently been reinforced by the adoption on October 7, 2019, of an EU Directive on "the protection of persons reporting on breaches of Union law" (the "EU Directive"). The purpose of the EU Directive is "to enhance the enforcement of

[European] Union law and policies in specific areas by laying down common minimum standards providing for a high level of protection of persons reporting on breaches." EU Member States will have two years after its publication in the Official Journal to transpose it into their national law. It is important to note that as of this writing, the EU Directive has not been made available and that as such, the information contained below is based on the latest version of the draft Directive, as agreed between the EU Parliament and Council on April 10, 2019 (referred to as "EU Proposal" below). As detailed below, the EU approach of the whistleblower protection seems to be more advantageous to whistleblowers than current regulations in France. Thus, when implementing the EU Directive, France will need, where appropriate, to introduce or retain the more favorable right of the reporting persons.

2. Scope

According to the definition set forth by Sapin II, a whistleblower entitled to a protection is an individual who discloses or reports, selflessly and in good faith: (i) a crime or a misdemeanor under French law; (ii) a clear and serious breach of an international commitment duly ratified or approved by France, of an act of an international organization pursuant to such engagement or of French laws or regulations; or (iii) a serious threat or harm to the public interest, of which he or she has personal knowledge. The French Constitutional Court (Conseil constitutionnel) highlighted that this definition was not restricted to employees and may also extend to external or occasional collaborators of the company. Despite the fact that whistleblowing technically falls outside of its mission scope, AFA's Recommendations also cover the topic, by indicating that there are five characteristics of a whistleblower: (i) he/she is an individual (not a legal entity); (ii) he/she has personal knowledge of the facts disclosed; (iii) he/she acts selflessly and (iv) in good faith; and (v) he/she discloses serious matters.

Contrary to the U.S. Dodd-Frank whistleblowing provisions, the French whistleblowing system is against any kind of financial incentive being provided for the benefit of the whistleblower. Not only is the whistleblower required to act "selflessly", as mentioned above, but he/she cannot be provided with any financial support. In fact, while the initial version of Sapin II provided that the Defender of Rights (Défenseur des droits) could grant, on the whistleblower's request, financial assistance, such possibility was invalidated by the French Constitutional Court (Conseil constitutionnel).

The EU Proposal thus appears to have a broader definition of the concept of whistleblower protection. Indeed, in the EU Proposal, neither personal knowledge of the breach, nor selflessness and good faith are requirements for whistleblower protection. On the one hand, Article 4.4 of the EU Proposal extends such whistleblower protection to colleagues or relatives connected with them and who may suffer retaliation in a work-related context. On the other hand, Recital 33 of the EU Proposal states that the motives of the whistleblower in reporting the breaches "should be irrelevant as to whether or not they should receive protection." In addition, Article 20.2 of the EU Proposal offers the possibility for Member States to provide for financial assistance and support to whistleblowers during legal proceedings.

3. Process

Sapin II provides that a whistleblower must follow a three-step reporting procedure in order to be entitled to protection. First, the whistleblower shall file a report to his or her line manager or employer or a person appointed for this purpose by the employer. In fact, private entities employing more than 50 persons are required to implement internal reporting procedures in order to enable their employees to initiate whistleblower alerts when necessary. Although no penalties are provided for failure to comply with such an obligation, companies must be aware that implementing a reporting system is in their best interests since, absent such system, they minimize the chances to keep a potential alert at the internal level (as opposed to the authorities and/or the public). Second, in the absence of an appropriate action undertaken within a reasonable time, where there is a serious and imminent

danger, or in the event of irreversible damages, the whistleblower may inform French judicial, administrative, or professional authorities. In this respect, the whistleblower may consult the Defender of Rights (Défenseur des droits) in order to be directed toward the appropriate authority. Third, and as a last resort in the absence of reaction from such authorities within a three-month period, the whistleblower may alert the public/report to the press.

Article 9.1.f of the EU Proposal limits the reasonable timeframe to provide feedback to the whistleblower to three months, whether the reporting was made through internal channels or to competent authorities. In addition, the EU Proposal appears to provide for more flexibility than Sapin II as to the types of reporting channels to be used by the whistleblower, as Article 10 of the EU Proposal offers whistleblowers the possibility to resort directly to external reporting channels.

4. Nature and extent of the whistleblower protection

If the above criteria for whistleblower status are met, then whistleblower status confers a protection under both criminal and labor law. With respect to criminal law, a whistleblower who breached a secret protected by law may benefit from criminal immunity under certain circumstances. With respect to labor law, the whistleblower will be granted a protection within the workplace. This protection makes it unlawful to exclude from or discriminate against a whistleblower in the recruitment process, internships, or professional training, to fire him/her, or to make him/her suffer any disciplinary sanctions as a result of having issued a signal or an alert. Any measure taken in violation of this protection will be null and void.

Article 19 of the EU Proposal does not limit retaliatory measures to the above-mentioned actions directly related to the employment contract. It includes for instance damage to the person’s reputation (particularly on social media), and financial loss, as well as blacklisting on the basis of informal or formal agreements, excluding the possibility for the person to find employment in a specific sector or industry in the future.

H. The Creation of an Obligation to Register as Representative of Interest

Under Sapin II, individuals engaged in lobbying in France, referred to as “representatives of interests,” must be listed in a dedicated National Registry kept by the Haute Autorité pour la Transparence de la Vie Publique (“HATVP” — High Authority of Transparency in Public Life) and follow particular ethics rules. Prior to these new provisions, disclosure of lobbying activities was done on an opt-in basis and applied only in the context of contacts made with parliamentarians. The provisions of Sapin II related to lobbyists entered into force as of July 1, 2018. As of the end of 2018, 1,734 individuals engaged in lobbying were listed on the National Registry and 6,362 lobbying activities were disclosed.

Lobbyists are defined under French statute as any natural person, as well as any private or public company, employing persons whose main activity is to influence public decision. This particularly includes influencing the content of laws and regulations by liaising with public officials, including members of the Government, members of the houses of Parliament, and certain local elected officials.

Lobbyists must disclose to the following information to the HATVP:

- For an individual, his/her identify; for a legal entity, the identity of its managers as well as its employees entrusted with lobbying activities;
- The scope of his/her/its lobbying activities;

- Acts in lobbying as well as the amount of expenses related to those activities in the previous year;
- The number of persons employed in carrying out its lobbying tasks and, as the case may be, the company's turnover for the previous years;
- Professional or trade union organizations or any association related to the represented interests to which he/her/it belongs.

Failure to comply with these obligations may be punished with a fine of up to 15,000 € and imprisonment of up to one year. The HATVP has the power to request documents and to conduct onsite verifications upon a judge's authorization, although any of the information collected in the context of its mission shall be treated as confidential. The HATVP also has the ability to control if the potential individuals engaged in lobbying are actually registered and if the registrants declared their activities properly. Following the HATVP statement in 2017 that the first declarations would not lead to any sanction, the authority confirmed that those received in 2018 can be controlled and sanctioned. In this perspective, the HATVP specified that the registrants need to be able to justify every elements disclosed and to document their analysis which lead to this disclosure.

The HATVP has observed a wide spectrum in terms of details and quality of the declarations received in 2018, which prompted the HATVP to conclude that there was a misunderstanding of some of the requirements, including the obligation to report on the nature of the activities. In order to enhance future declarations, the HATVP launched two working sessions in mid-July 2018. It emerged from these sessions that confusion surrounding the declarations arose from the complexity and time consuming nature of reporting scheme. In this regard, the HATVP confirmed through public statement that the difficulties of the reporting scheme are due, in part, to the objectionable legal definition of "representatives of interest", which is both too wide and too narrow, thus complicating the declarations. As of the time of this Alert, there has not been specific action taken to address this criticism.

Lobbying registration requirements also exist at the European level, however such registration is non-mandatory (except for members of the European Parliament) and is encouraged by various incentives. Companies which register themselves on the European Transparency Register (which covers lobbying activities with both the European Commission and the European Parliament) by providing information on their organization's objectives, mission, structure, activities, and legal status, and which agree to the applicable Code of Conduct of the Transparency Register, can benefit from various advantages such as (i) long-term access to the premises of the European Parliament; (ii) eligibility as a speaker at public hearings held by parliamentary committees; (iii) supporting or participating in activities of Parliament's intergroup or unofficial grouping; (iv) meeting with European Commissioners, Cabinet members and Directors-General; and (v) participating in public consultations and having contacts with civil servants at the European Council. As of today, the three EU institutions, which include the European Parliament, the European Commission and the Council of the European Union continue their discussions on moving towards a joint mandatory Transparency Register. The last round of talks in this regard were held on February 13, 2019.

II. Enforcement Action: the Cour de Cassation's ruling in the Oil for Food Case

With its new anti-corruption landscape, there are good reasons to believe that prosecutions as well as convictions based on corruption of foreign officials, will increase in France. Prior to the recent Oil-for-Food precedent (discussed herein), the only conviction of a French company (Safran) for corruption of Nigerian public officials had been overturned by the Paris Court of Appeals in 2015. Whether this case law (and the increased CJIP activity discussed above) signals the beginning of a new and active enforcement environment in France remains to be seen.

On February 26, 2016, the Paris Court of Appeals held that Total and Vittol, two French companies, were guilty of corruption of foreign public officials in the context of the United Nations' "Oil-for-Food Program" and imposed fines on each of the companies in the amounts of 750,000 € and 300,000 €, respectively. On March 14, 2018, the Criminal Section of the *Cour de Cassation* (decision No. 16-82117) issued the latest ruling in the "Oil-for-Food" scandal. Long and complex, this decision notably confirmed the Paris Court of Appeal's decision in that it sentenced some of the defendants for active corruption of foreign public officials. Beyond that, the case is worth some analysis in that it may provide guidance and have consequences on future prosecutions of corrupt acts in France.

A. Background of the case

Following the invasion of Kuwait by Iraq in early August 1990, the United Nations (UN) established an embargo regime that prohibited the provision of funds or resources to the Iraqi government. However, due to difficulties faced by the Iraqi population, the UN Security Council adopted Resolution No. 986 on April 14, 1995 in order to ease this embargo by allowing Iraq to sell oil, provided that certain conditions were met. These conditions, framing the so-called "Oil-For-Food Program," required the State Organization for the Marketing of Oil ("SOMO"), a state-owned company attached to the Iraqi Ministry of Petroleum, to sell petroleum at a given price set below the oil market price and paid into an escrow account under UN control, which was meant to ensure that the funds were used to acquire food and basic necessities by the State.

However, from 2000 onwards, the Iraqi regime applied a "tax" or "surcharge" on sales worth 10% of the value of a barrel, in violation of UN Resolution No. 986. The companies were required to pay the surcharge by the Iraqi Revolutionary Command Council, holding both executive and legislative powers in the country, if they wanted to pursue their commercial relations with SOMO and continue buying oil in Iraq. While the funds corresponding to the price set by the UN were to be transferred to the escrow account, companies were required to pay the "surcharges" either: (i) into accounts opened in Jordan or Lebanon in the name of SOMO, its officers, or Iraqi officials, or (ii) in cash at various Iraqi embassies. Such transfers were by definition neither controlled nor approved by the UN.

B. Narrow scope of the ne bis in idem principle

In the first instance, the *Tribunal Correctionnel* notably considered that one of the defendants (Vitol) could not be prosecuted in France, pursuant to Article 14(7) of the 1966 International Covenant on Civil and Political Rights (ICCPR), under a theory of *ne bis in idem*, which prohibits the prosecution or conviction of a person twice for the same act. In fact, in November 2007, this defendant had already entered into a plea deal in the New York State court for the same facts. As for the other defendants, the judges of first instance considered that the components of the offences at stake were not sufficiently characterized.

With respect to this question, the Court of Appeals considered that while Article 14(7) of the ICCPR may apply to multi-jurisdiction prosecutions, the settlement reached in the U.S. and the charges in France were different. Indeed, defendants were charged in France with "active corruption of foreign public official," while Vitol's guilty plea in the U.S. covered "grand larceny."

The Cour de Cassation, after asserting that Article 14(7) of the ICCPR only applies to cases "whereby the two proceedings have been initiated on the territory of the same State," considered that the transnational principle of ne bis in idem was non-applicable in the present case, although a plea bargain had already been reached by the concerned defendant in the U.S. In line with its longstanding case law, the Cour de Cassation held that ne bis in idem does not apply in situations where a French court's jurisdiction over the matter is territorial (compétence

territoriale). In fact, while Article 113-9 of the French Code of Criminal Procedure provides that "no prosecution may be brought against a person who establishes that he was subject to a final decision abroad for the same offence (…)," "in the cases set out under Articles 113-6 and 113-7," i.e., when the offense was committed as a whole outside French territory, no such limitation is set forth within the law when the offence was committed, even partly, in France. This longstanding principle can be explained by the French courts' attachment to their sovereignty over criminal cases committed on their territory, which they will not yield in the face of foreign decisions. This decision is consistent with other case law rendered by the same Cour de Cassation on January 17, 2018, which involved the CEO of a Gibraltar company who had bribed Nigerian authorities in the context of a public procurement. In that case, although a plea agreement had been concluded in the U.S. by the CEO and the U.S. DOJ had concluded its investigations in the country, the Cour de Cassation had set aside the settlement. According to the Cour de Cassation, the transnational principle of ne bis in idem could not apply since part of the facts at stake had been committed partially on the French territory, which thus enabled the executive's prosecution in France.

C. Broad interpretation of the concept of "corrupt person"

The *Cour de Cassation* approved the appellate court's reasoning that the surcharges were beneficial to the Iraqi government, noting that no article in the OECD Convention of 1997 excluded a State from being considered as a beneficiary of corruption (even though it also did not explicitly define it as such). According to the *Cour de Cassation*, Article 435-3 of the French Criminal Code, as worded at the time of the facts, covered the situation whereby a person yields to unlawful requests "*from agents of a body having the status of a person entrusted with a public service mission,* (…) *conveying requests for payment of hidden commissions made by a State's representative bodies, which are its final beneficiaries*."

Applied to today's wording of Article 435-3 of the French Criminal Code, which applies to advantages promised to a government official "either for his/her own benefit or that of a third party," the decision of the *Cour de Cassation* decision can be read to mean that the "third party" under the French Criminal Code may be a State.

D. The extensive scope of the concept of "Illicit payments"

The defendants argued that the offence of corruption of foreign public officials could not be characterized because Article 435-3 of the French Criminal Code required that offers, promises, donations, gifts, or benefits be requested "without right" (*sans droit*). The defendants argued that, based on the OECD Convention, which provides that "*it is not an offense if the advantage was permitted or required by the written law or regulation of the foreign public official's country, including case law*," the surcharges they were paying to the Iraqi regime resulted from a decision made by the Iraqi Revolutionary Command Council, holding both executive and legislative powers in the country at that time, and circulated through various memoranda to the different Ministries.

The *Cour de Cassation* sided, however, with the Paris Court of Appeal by stating that "it [had] not been established [by the defendants] that the hidden surcharges, whose payments were requested by Iraqi State agents outside of the scope of the market organized by UN Security Council Resolution No. 986 of April 14 1995, were permitted or required by the written law or regulations of the Iraqi State." By doing so, the *Cour de Cassation* reversed the burden of proof, requiring that the defendants prove that such surcharges were permitted by the written laws or regulations of the Iraqi State. This appears to be consistent with the prosecutors' position, which considers that there is a presumption of impropriety to advantages given or offered to foreign officials. In any case, the *Cour de Cassation* followed the Court of Appeal's reasoning, when it considered that international transactions in Iraq were at the time governed by Resolution No. 986, which forbid such surcharges, as Iraq was a failed State, and could not adopt proper legislation to translate the Resolution into law.

III. Other Related Legislative Initiatives

France has recently adopted other legislative initiatives aimed principally at increasing transparency among businesses to prevent corruption and also to require companies to prevent environmental and human rights violations within their control. These laws include the "Devoir de Vigilance" ("Obligation of Vigilance") and the implementation of the Fourth European Anti-Money Laundering Directive. More generally, France also enacted a law extending the statute of limitation for felonies and misdemeanors.

A. Devoir de Vigilance

1. Background

Following a lengthy debate first initiated in 2013, the Devoir de Vigilance law ("Duty of Vigilance Law"), passed on February 21, 2017 and was enacted on March 27, 2017 after having been assessed by the Constitutional Council on March 23, 2017. The law introduces a new principle of a duty of care for companies with respect to their subsidiaries, suppliers, and subcontractors. The bill is intended to enhance the implementation of the United Nations Guiding Principles on Business and Human Rights – the global reference framework on corporate social responsibility – and received strong popular support. It was proposed in response to a series of human rights violations committed by large companies, specifically the 2013 structural failure of Rana Plaza in Bangladesh, a tragedy which resulted in over 1,000 employees being killed in the collapse of an eight-story commercial building. The law was nonetheless subject to significant debate, with the French Senate considering that the bill would place a significant and unique burden on French companies, and would place them at a commercial disadvantage compared to their competitors. Opponents of the text also considered such a law to be unnecessary in light of the Directive 2014/95/EU that already requires large entities to disclose information regarding their Corporate Social Responsibility policies. The Duty of Vigilance Law nonetheless finally enacted on March 27, 2017, and imposes several obligations on the companies that are subject to it.

2. Scope

The Duty of Vigilance Law applies to companies incorporated in France that have at least 5,000 employees, including in their direct and indirect French subsidiaries, or which employ over 10,000 individuals including in their foreign direct and indirect subsidiaries. Hence, it is estimated that only large companies – approximately 150 to 200 French entities – are directly covered by this law. Under the law, companies must create risk mitigation plans (plans de vigilance) designed to monitor companies' supply chains in order to prevent serious damages to (i) human rights and fundamental freedoms; (ii) health and safety, and (iii) the environment. These risk mitigation plans must be developed by the companies targeted by the law, and must cover the activities of their affiliates, subsidiaries, as well as those of their suppliers and subcontractors with whom they have established business relationships, both in France and abroad. As a result, even though the Duty of Vigilance Law technically imposes obligations only on large French companies, smaller companies will also be impacted if they are affiliates, subsidiaries and even suppliers or subcontractors of companies subject to the law.

3. Obligations

Companies subject to the law must not only develop the risk mitigation plan, but they also have the obligation to implement it effectively, and to publish the plan along with a report on its implementation. The risk mitigation plan shall include: (i) a risk mapping intended to identify, analyze and rank the risks; (ii) due diligence and risk assessment procedures to be conducted on subsidiaries, subcontractors and suppliers; (iii) appropriate actions of risk mitigation and prevention of serious damages; (iv) a whistleblowing procedure allowing the collection of

relevant information in light of the risks targeted; and, (v) a follow-up and assessment mechanism of the measures undertaken in response to the risks identified. Given the similarity of the mechanisms and measures required under the Duty of Vigilance Law and Sapin II, companies subject to both laws may wish to consider merging their processes to avoid duplication and inconsistencies.

4. Enforcement in practice

As of the time of this Alert, four Duty of Vigilance notices had been issued: two against the oil & gas company Total, respectively in October 2018 and June 2019, one in July 2019 against Teleperformance, a company in the business of operating call centers and the latest one in early October 2019, against the electricity supplier EDF. All claimants of these notices included French associations with activities focusing on human rights and environmental issues. The first notice against Total was issued on the basis of an allegedly incomplete risk mitigation plan reportedly failing to address the adverse impact on climate change from the company's greenhouse gas emissions. Total responded within the three-month period required by the law, explaining (i) that it takes into account climate change in its activities, particularly in annual reports published since 2016 on the integration of climate in their strategy, and (ii) that despite their belief that risks related to climate change do not fall within the risk categories covered by the Duty of Vigilance Law, they nonetheless plan to address this topic in their 2019 management report (which will include the risk mitigation plan). The second notice against Total was issued by four Ugandan associations and two French associations, in connection with an oil project in Uganda. These associations claim that there are serious risks involving human rights and the environment that have not been addressed in Total's mitigation plan. Total also responded to this claim within the appropriate time-limit, by denying the allegations and explaining that its risk-mitigation plan complies with its obligations under the Duty of Vigilance Law. The associations have threatened additional legal action against the company, but as of the writing of this Alert, no such action appears to have been initiated. The notice issued against Teleperformance, is based on the alleged absence of publication of a risk mitigation plan for the year 2018, and on the publication of a two-page risk mitigation plan for the year 2019, despite allegations of human and fundamental labor rights abuses in a Colombian call center reported in July 2019 by UNI Global Union. The latest notice filed on the basis of the Duty of Vigilance Law was issued against EDF for its alleged failure to respect the free prior and informed consent of Mexican indigenous communities in connection with the construction project of a 300-megawatt windfarm led by its Mexican subsidiary in the Oaxaca State.

5. Trends identified with respect to risk mitigation plans' content

A few studies and reports were published by French associations and NGOs in order to assess the content of the first risk mitigation plans published so far. One of them, published in February 2019 (the February 2019 Report) by a group of four NGOs (Amis de la Terre, Amnesty International, CCFD-Terre Solidaire, and Collectif Éthique sur l'étiquette) reviewed 80 risk mitigation plans, while another report published in June 2019 (the June 2019 Report) by the association Entreprises pour les droits de l'Homme based its assessment on the review of 83 risk mitigation plans.

According to the findings of the February 2019 report, companies could "do better," notably in terms of (i) comprehensiveness of the plan (its scope, especially the activities of suppliers and subcontractors, is generally not clearly defined); (ii) methodology of the risk-assessment (the shift from assessing risks for the company itself to assessing risks for external stakeholders has not been made yet), and (iii) responses to the risks identified (they should be more precise than the general policies and voluntary commitments often provided).

According to the findings of the June 2019 Report, most risk mitigation plans are now formalized and the challenge mainly consists of implementing such plans throughout the affiliates and subsidiaries of the companies that developed them. To this end, one-fourth of the companies reviewed reportedly put in place a steering

mechanism and one-third appear to ensure follow-up on the implementation of the plans by the company's governing bodies. Human rights risk-assessments appear to have been reinforced in 2018, with responses more adapted to the risks identified. Responsible procurement policies are also being adapted to the requirements of the law with a better identification of the risks. In other words, companies need to progress to comply adequately with the requirements of the Duty of Vigilance Law, but they are still in a learning phase given the relative recency of the law.

B. Anti-Money Laundering

France's tools to combat money laundering and counter terrorism financing ("AML-CTF legislation" hereinafter) center around the general offense of money laundering. The detection of illicit financial flows also relies on due diligence requirements imposed on certain professions and organizations. The French AML-CTF regulations combine repressive and preventative aspects which are primarily found in the French Criminal Code and the French Monetary and Financial Code ("FMFC"). The French Criminal Code directly prohibits money laundering and terrorism financing; the French Monetary and Financial Code imposes an obligation on targeted entities ("Subjected Entities") to implement an AML-CTF framework.

On December 1, 2016, France implemented the fourth European Anti-Money Laundering Directive via Ordinance No. 2016-1635 to strengthen existing anti-money laundering and terrorism financing legislation in France. The transposition into French law in the upcoming months of the fifth European Anti-Money Laundering Directive adopted by the European Parliament on May 30, 2018 shall contribute to the reinforcement of France's AML-CTF framework.

The French AML-CTF framework also includes two central pillars: the obligation to conduct due diligence on their clients, and the obligation to report suspicious transactions to the French Financial Intelligence Unit ("*TRACFIN"*).

1. The expansion of the AML-CTF legislation scope

In December 2016, the scope of entities subject to AML-CTF legislation was expanded to include not only financial service companies, but also non-financial service companies trading in precious stones, fine metals, jewels, furniture, interior decorative items, cosmetics, textile products, leather goods, fine foods, clocks, and tableware, accepting payments in cash above an amount set by a 2018 decree at 10,000 €. In addition, the French Monetary and Financial Code (Code monétaire et financier) now specifies that AML-CTF requirements embrace both legal and natural persons falling into the listed categories.

Although they relate to money laundering, the AML-CTF requirements are somewhat similar in structure to the anti-corruption measures and procedures required by Sapin II, and include: (i) a risk assessment; (ii) policies adjusted to the risk assessment; (iii) internal controls and procedures; (iv) a person in charge of implementing the AML-CTF compliance program who must be sufficiently senior in the hierarchy and understand the AML risk faced by the company; and (v) adjustments to the recruitment policy. When entities subject to the legislation belongs to a group of companies and their headquarters are located in France, they must implement AML-CFT compliance program at the group level (including their subsidiaries in France) and share information among the other companies in the group.

Companies that are subject to the laws are required to conduct certain verifications on their customers before entering into a business relationship, including verifying their identity and their ultimate beneficial owner. This requirement must also be performed for occasional customers when a red flag arises. When the risk appears to be low and normal business activity would otherwise be interrupted, such verification can be performed during the

business relationship instead of before. Various levels of verifications are set by the law depending on the risks. In particular, they must set up internal risk-based mechanisms to identify whether customers are politically exposed persons (PEPs) as defined by French law and perform supplemental verifications on such customers. In instances where a breach of the AML-CFT laws are identified, sanctions may also be imposed on directors, employees and persons acting on behalf of the entity in question, if such individuals are found to have been personally involved in the conduct.

In 2017, the French banking authority (Autorité de Contrôle prudentiel et de résolution or "ACPR") fined the French banks BNP Paribas and Société Générale respectively 10 million € and 5 million € for inadequate money-laundering controls. In 2018, the ACPR performed 1,300 off-site document reviews ("contrôle sur pièce") and 29 onsite controls ("contrôle sur place"), 8 of which resulted in recommendations and 9 in disciplinary actions. Among these 9 disciplinary actions brought by the ACPR Sanction Committee, two stood out. The first was brought against CNP Assurance and the second against La Banque Postale which were respectively fined 8 million € and 50 million € for deficiencies in their AML-CTF framework.

2. ACPR publications

In 2018 and 2019, the ACPR, in association with the French Treasury (Direction Générale du Trésor or "DGT") and TRACFIN published/updated the four guidelines below relating to:

- **Filing of suspicious activity reports ("SAR") to TRACFIN:** on November 5, 2018, the ACPR and TRACFIN published their updated guidelines on the obligation to file a report to TRACFIN when suspicious activity is identified. This new guidance came only a few months after the last update on February 2018, in order to include the provisions of Decree No. 2018-284 dated April 18, 2018. This last updated version notably shed light on the obligation to accurately characterize within the report the suspicious facts leading to the filing of a SAR;

- **Clients' identification:** on December 14, 2018, the ACPR published guidelines relating to the due diligence to be conducted by Subjected Entities on their clients up to their beneficial owner(s). These guidelines merge the guidelines on business relationships and occasional clients last revised in 2013 and the ones relating to the ultimate beneficial owner issued in 2011. These guidelines describe the extent of the due diligence (information and supporting evidence) to be conducted on clients in the KYC process depending on the nature of the client and the nature of the business relationship between the Subjected Entities and the client (i.e., "clients in an established business relationship"/"occasional clients");

- **AML-CTF and asset-freeze reporting:** pursuant to a Decree issued on December 21, 2018, the ACPR clarified in its March 21, 2019 guidelines, the content of the AML-CTF and asset freeze internal control audit report that banking and life insurance institutions are required to file annually to the ACPR. These annual reports provide an evaluation of the efficiency of the implemented internal controls systems and processes relating to AML-CTF and asset-freeze;

- **Asset-freeze:** the ACPR and the DGT updated their joint guidelines on asset-freeze obligations on June 6, 2019, to include the modifications of the asset freeze framework pursuant to Ordinance No. 2016-1575 dated November 24, 2016 and Decree No. 2018-264 dated April 9, 2018. These guidelines describe the various sources of existing asset-freeze measures (UN, EU and National). They also provide specific advice on how Subjected Entities shall implement a dedicated framework to detect, prevent and report any transaction relating to these targeted individuals and entities.

The ACPR also published an AML-CTF report on September 2019 relating to the oversight of AML-CTF systems and processes in the banking and insurance sectors based on its assessments and controls of various banks and insurance groups between 2016 and 2018. This report highlights the weaknesses and suggested improvement in the following five key AML-CTF areas: (i) governance, (ii) policies and procedures, (iii) supervision at Group level of foreign activities conducted by branches and subsidiaries, (iv) sharing of information within the Group and (v) internal controls. The ACPR noted that AML-CTF supervision at Group level was often unsatisfactory. Throughout its controls, the ACPR stressed the importance of a centralized AML-CTF function at Group level to overview the consistency and efficiency of AML-CTF systems and processes. The ACPR expects parent companies to elaborate an AML-CTF risk classification integrating each of the branches' and subsidiaries' exposure levels and to consequently have these branches and subsidiaries implement local AML-CTF procedures and processes (reflecting at the very least the parent company requirements). The central AML-CTF function should also actively monitor the local implementation of the AML-CTF framework to ensure that it is fully consistent with the parent company's standards. The ACPR report also emphasizes that sufficient means (human and financial) need to be allocated to the monitoring of the AML-CTF framework and to the training of the employees. The report finally highlights that information sharing is paramount to robust AML-CTF systems and processes and also stresses the importance of an efficient internal control framework at Group level.

3. Public record of Ultimate Beneficial Owners (UBO)

Since the adoption of an ordinance in December 2016, as modified in June 2017 and April 2018, French and foreign companies and corporations were required to identify and register their "ultimate beneficial owner" by August 1, 2017, and must file certain information about those ultimate beneficial owners by April 1, 2018.

An ultimate beneficial owner is broadly defined under French law and can include one or more individuals who ultimately own or control the company or the corporation, or on whose behalf a transaction or an operation is conducted. An individual is considered to own or control the company or corporation if the person holds, directly or indirectly, at least 25% of the share capital or voting rights of the subjected company or corporation. An individual or individuals can also be considered an ultimate beneficial owner when it effectively determines the decisions taken at that company's general meetings through the voting rights it holds or by holding the power or when it is a partner in, or member or shareholder of that company and has the power to appoint or dismiss the majority of the members of that company's administrative, management or supervisory organs.

The law applies to companies and corporations with a registered office in France, foreign companies with a branch in France, and other legal entities that are required to register in France under legislation or regulations. Companies listed on a regulated market in France or in another EU member state that is a party to the European Economic Area agreement, or in a country imposing similar requirements (such as the United States NYSE) are not subjected to this requirement.

Entities subject to the new rules must obtain and keep accurate records of their beneficial owner or owners, must provide this information to the commercial registry upon registration, and then must provide regular updates should the content of the information filed change.

4. Reinforcement of the French Financial Intelligence Unit's prerogatives (TRACFIN)

Created in 1990, TRACFIN (Traitement du Renseignement et Action contre les Circuits Financiers clandestins*,* or Unit for Intelligence Processing and Action against Secret Financial Channels) is a French agency aimed at fighting clandestine financing channels, money laundering, corruption, and terrorism financing. Certain individuals

and organizations (such as financial institutions, auditors, and insurance companies) are required by law to declare suspicious and potentially corrupt activity, and TRACFIN centralizes and analyzes these declarations. More than half of the investigations into corruption in France are started after the filing of a report of potential misconduct before TRACFIN. If, during the analysis of the information provided, TRACFIN determines that there are indications of corrupt activity, the agency may refer the matter to the prosecutor or to special investigation services.

In December 2016, TRACFIN's powers were expanded. TRACFIN is now vested with the authority to identify any entity subject to its reporting obligations, including any financial operations or persons that may present a high risk of money laundering or financing of terrorism. In addition, TRACFIN's right to postpone the execution of any pending suspicious transactions has been increased from five to ten working days. TRACFIN is also now authorized to communicate collected information to several administrative authorities (including customs, tax administration, financial jurisdictions, and the AFA).

In 2018, 79,376 "pieces of information" were transmitted to TRACFIN, including 76,316 Suspicious Activity Reports or "SAR", amounting to a 12% increase since 2017, and a 75% increase in three years, which may be a result at least in part of its expanded powers. In ten years, the number of "pieces of information" received has been multiplied by 5. TRACFIN conducted investigations or posed further questions on 14,554 of those reports in 2018 (a 16% decrease compared as compared to 2017), and 2,255 investigation requests were sent to foreign investigatory counterparts. TRACFIN sent 3,282 files to French judicial and administrative authorities (a 26% increase since 2017) for further action based on its analysis of reports of suspicious activity.

C. The Potential Reinforcement of the French Blocking Statute

The question of the French Blocking Statute, first implemented in 1968 (and revised in 1980) to protect France's economic interests, has been revived with the release, in June 2019, of the "Gauvain Report" (after the name of the French MP, Raphael Gauvain, who was in charge of conducting the underlying study), more officially titled "Restore the sovereignty of France and Europe and protect our companies from laws and measures with extraterritorial scope" ("Gauvain Report"). Starting with the preliminary observation that the vast majority of foreign companies convicted of corruption in the U.S. in recent years are European and, more specifically, French, and that the underlying proceedings led foreign prosecution authorities to collect information on such companies in order to allegedly serve economic purposes, the report comes to the conclusion that "*French companies do not currently have effective legal tools to resist legal actions launched against them, be it by competitors or foreign authorities*". Among the defective mechanisms, the Gauvain Report cites the French Blocking Statute, which prohibits any person from requesting, seeking or disclosing, in writing, orally or in any other form, documents or information of an economic, commercial, financial or technical nature when such communication is (i) capable of harming the sovereignty, security or essential economic interest of France of contravening public policy and/or (ii) directed toward establishing evidence in view foreign judicial or administrative proceedings or in relation thereto, unless such information is communicated through a treaty, international agreement, or other applicable laws or regulations. The idea behind the Blocking Statute was to require foreign authorities to make formal requests for such information through French authorities, and allow French authorities to in turn control the flow of sensitive information outside of France. The Gauvain Report, however, indicates that the French Blocking Statute has been largely ineffective, citing the fact that the applicable sanctions (fine of up to 18,000 € (and up to 90,000 € for legal entities) and/or to an imprisonment sentence of up to six months) are insufficient and the statute has been rarely applied (with only one case of sanction since its enactment – Criminal Chamber, 12 December 2007, No.07-83228) conduct the statute to be regularly disregarded by U.S. and other foreign (such as in the U.K.) Tribunals (*See* e.g. *Société nationale industrielle aérospatiale v. United States District Court for the Southern District of Iowa,* 15 June 1987).

In order to reinforce the French Blocking Statute, the Gauvain Report suggests:

- Imposing a mandatory reporting of foreign requests for information and entrusting the SISSE (“Service de l'information stratégique et de la sécurité économiques” or Strategic Information and Economic Security Service, an administration placed under the authority of the French Ministry of Economy) to handle those reports, with sanctions in the event of default of up to 50,000 € and / or 6 month’s imprisonment;

- Substantially increasing the sanctions for violation of the French Blocking Statute from 18,000 € to 2 million € (and up to 10 million € for legal entities) and two years’ imprisonment;

- Implementing a support program for companies which make a report to the SISSE, whose role would notably be to assess the scope of confidential information that could be requested by the foreign authority, to inform the company of the risks and to communicate with the foreign authority in order to remind it of the terms of the French Blocking Statute and the appropriate channels to be used to obtain the requested information;

- Creating specific rules framing the compliance monitoring program of a French company imposed by a foreign court’s decision – which should be appropriately assessed in light of the AFA’s existing competence in this area – and

- Insuring that the French Blocking Statute of 1968 does not prevent cooperation with foreign authorities or otherwise encourage violations of international agreements.

In the same vein, the Gauvain Report also recommends regulations surrounding the transmission of information and numeric data of legal entities by hosting providers to foreign judicial and administrative authorities related to French natural persons, French legal entities or French residents. These recommendations appear aimed at helping companies protect themselves from the Cloud Act, to which the Gauvain report suggests:

- Forbidding the transmission of information and numeric data of the legal entity without going through the official channel, based on the model of the French Blocking Statute;

- Creating a dissuasive administrative fine: a maximum amount of 20 million €, or in a case of a company, 4% of the company’s total annual global turnover, whichever is greater. This sanction is similar to the provision 83-5 of the GDPR. This fine would take into account different criteria such as (i) the damages caused to the economy; (ii) the nature of the transmitted information and numeric data; (iii) the gravity and frequency of the violation and (iv) any precedents. The third measure is the designation of an administrative entity which would be in charge of sanctioning any infringement.

- Entrusting the French Telecommunications Regulation Authority (“Autorité de Régulation des Communications Electroniques et des Postes” or (“ARCEP”)) with controlling, investigating, and sanctioning (or settling with) the subjected entities.

Other proposals of the Gauvain Report consist of the following:

- Creating a status for French in-house lawyers in order to protect the confidentiality of in-house legal opinions and subject it to legal privilege, which would seek to provide in-house lawyers for

French companies with the same level of protection and confidentiality as their main foreign counterparts (i.e., U.S. or U.K. in-house counsels, who benefit from legal privilege protections);

- elaborating a shared national doctrine related to secrets essential to the economic interests of France;
- ensuring a clearer understanding of the prosecutor's criminal policy with respect to the implementation of the CJIP;
- reinforcing the multilateralism of extraterritorially by two French initiatives before the International Court of Justice and the OECD consisting of (i) referring an opinion to the International Court of Justice to establish an international law regarding extraterritoriality and (ii) launching a discussion on extraterritorial laws at the OCDE;
- elaborating a French proposal to the EU blocking statute to reinforce European tools for the protection of European companies facing requests from non-EU administrative or judicial authorities; and
- requesting a parliamentary report to strengthen the tools and means to fight against economic and financial crime, in particular the corruption of foreign officials.

Chapter 5: Anti-Corruption Enforcement Updates In Select Countries

The most drastic developments in the area of anti-corruption enforcement continue to come from unexpected sources. Chapter 5 includes highlights from Brazil, China, and Mexico.

For a number of years, observers could be forgiven for concluding that anti-corruption enforcement was primarily an American activity, and that the FCPA enforcement was the primary—if not only—anti-corruption risk faced by companies. The world is different today.

Below we explore anti-corruption enforcement developments in Brazil, China, France, Mexico, and Norway.

I. <u>Brazil</u>

A. Introduction

Since the beginning of "Operation Car Wash," Brazil has maintained its position as a major player in the global fight against corruption. The U.S., DOJ, and SEC reportedly have dozens of open investigations with connections to Brazil, including probes into Brazilian companies across various industries (e.g., food, power/energy, oil and gas, steel, air transport, telecommunications and banking) and foreign companies operating in Brazil. Moreover, Brazil continues to cooperate in cross-border corruption investigations, including with enforcement colleagues in the U.S., France, Switzerland, U.K., Singapore, Argentina and elsewhere.

Brazil's political atmosphere has had a significant impact on its fight against corruption. Conversely, the fight against corruption has had a significant impact on Brazil's political atmosphere. In the 2018 elections, the conservative candidate Mr. Jair Bolsonaro won the presidency on an anti-corruption platform and appointed Mr. Sérgio Moro, the main judge overseeing the Car Wash cases, as Minister of Justice, one of the main cabinet positions in the executive branch.

Below we highlight the most relevant efforts by Brazilian enforcement authorities over recent years. In addition, we examine Brazil's anti-corruption framework, including the Clean Companies Act and newly issued guidelines and regulations on investigations, as well as the negotiation and implementation of corporate settlements.

B. Enforcement Highlights

1. Operation Car Wash

Operation Car Wash remains the largest anti-corruption campaign in Brazil's history. It started in 2014 as a small-scale probe into illegal currency exchange and money laundering. Its scope rapidly expanded over the years as Brazilian authorities uncovered evidence of a massive bribery scheme. While, in the early phases, Operation Car Wash focused mostly on allegations involving Brazil's oil company Petrobras, the probe has since widened to cover conduct by many other state-controlled companies. Notably, the largest EPCI groups in Brazil allegedly colluded to rig bids and fix prices, paying kickbacks to public officials who not only failed to halt the cartel, but also actively favored its members.

As of July 2019, the escalated enforcement efforts from Operation Car Wash in the southern city of Curitiba included: (i) 2,476 investigations and enforcement actions against companies and individuals related to allegations of bribery, money laundering, and conspiracy; (ii) 322 arrests; (iii) 195 settlements (including leniency agreements with companies and plea bargains with individuals); and (iv) 754 international cooperation proceedings (including active and passive requests). Operation Car Wash has also led to investigations and enforcement actions in three other Brazilian cities, Brasília, Rio de Janeiro and São Paulo. Brazilian authorities are reportedly seeking to recover a total of BRL 49,01 billion ($13 billion), including fines, as well as funds misappropriated from Petrobras through procurement fraud, inflated prices, and unjustified contract amendments.

A significant part of the investigation is confidential; therefore, the probe is likely to produce further developments in the near future.

Individuals investigated and arrested in connection with Operation Car Wash include high-level company executives, commercial agents, Petrobras officials, and Brazilian politicians, including former presidents, cabinet members, federal congressional representatives, and senators from the entire political spectrum. Over the past three years, some of Brazil's most prominent political figures have been charged with and convicted of corruption in the scope of Operation Car Wash.

In June 2017, Brazil's Prosecutor-General presented corruption charges against then-President Michel Temer (Brazilian President following the impeachment of Dilma Rousseff in 2016 to December 2017) for allegedly receiving bribes through an agent to influence a decision by Brazil's antitrust agency (CADE). Since the House of Representatives must authorize the indictment of a sitting president under Brazilian law, Mr. Temer was able to stall formal prosecution with the help of his coalition in Congress. However, after leaving office in December 2018, Mr. Temer was arrested twice over allegations of corruption in connection with Operation Car Wash. He was released from provisional arrest in May 2019 and currently awaits trial.

In July 2017, former President Luiz Inácio Lula da Silva (in office from 2003-2011) was convicted of corruption and money laundering for allegedly receiving bribes from EPCI giant OAS in order to influence the award of certain Petrobras contracts. He was initially sentenced to nearly 10 years in prison by lower court judge Sérgio Moro. In April 2018, the appeals court upheld the conviction and increased the penalty to approximately 12 years. However, in April 2019, the Superior Court of Justice reduced Lula's sentence to 8 years and 10 months. Following the sentence reduction, Lula became eligible for progression to the semi-open prison regime, which, in practice, may allow him to serve the remainder of his sentence under house arrest.

In April 2018, the Supreme Court ruled that then-Senator Aécio Neves, the former president of the right-wing Brazilian Social Democratic Party (PSDB), and a former presidential candidate, should stand trial for corruption and obstruction of justice. The Federal Public Prosecutor's Office presented charges against Aécio Neves in 2017. Aécio Neves was recorded by executives of meatpacking giant JBS soliciting a BRL 2 million bribe from JBS's Chairman. The delivery of the funds was subsequently confirmed (and filmed) by the Federal Police. The recordings were handed to Prosecutors by the JBS executives in connection with their plea bargain agreements.

2. Operation Car Wash's recent setbacks

While there is still public support for the investigation, Operation Car Wash has raised criticism from its opponents about potential judicial abuses and political bias, and has faced several recent setbacks. Since June 9, 2019, a news website (*The Intercept*) has published a series of exposés with excerpts of leaked text messages exchanged between then-Judge Sérgio Moro and Operation Car Wash prosecutors, as well as among the public prosecutors. Critics suggest that the messages provide evidence that Judge Moro engaged in unethical and unlawful coordination with the prosecutors and that the operation has a political agenda. Although those allegations have been highly disputed, the leaked messages have affected the credibility of Operation Car Wash.

Recent developments in the three branches of government have further destabilized the Car Wash probe. On the legislative front, in September 2019, Congress passed a law criminalizing abuse of power by prosecutors and judges. With respect to the executive branch, the newly elected President Jair Bolsonaro has been criticized for having taken an increased role in high-level appointments to the Federal Police, the Internal Revenue Service and the Financial Activities Control Council ("COAF"), after these agencies launched money-laundering investigations against the President's son. Finally, with respect to the judiciary, three Supreme Court rulings had a strong impact on Operation Car Wash enforcement efforts. In March 2019, Brazil's Federal Supreme Court ("STF") held that

corruption investigations involving illegal campaign donations (the so-called "*caixa 2*," *i.e.,* slush funds) should be tried by electoral courts, which, according to critics of the decision, are ill-equipped to conduct criminal proceedings at an appropriate speed. In addition, in July 2019, the STF's Chief Justice granted the petition of the President's son to suspend all ongoing investigations based on confidential data shared by COAF without prior judicial authorization. The ruling had the effect of paralyzing most money-laundering investigations in Brazil. Moreover, in August and September 2019, the STF overturned two convictions of Petrobras executives (Petrobras' former president Aldemir Bendine and another senior manager) on procedural grounds. These were the first Car Wash convictions to be overturned by the STF on such grounds, but several more could follow.

C. Anti-Corruption Laws

Brazil completely overhauled its anti-corruption framework with the enactment of the Clean Companies Act ("CCA") (Law No. 12846/13) in January 2014. Under the CCA, companies are subject to a strict liability standard for bribery and fraud against domestic and foreign public institutions, risking harsh punishment regardless of corrupt intent. Notably, potential sanctions may include monetary fines, ranging from 0.1 to 20% of the company's latest annual gross revenues, or, when these are undetermined, up to R$60 million (equivalent to approximately $15 million), as well as debarment from public procurement, and even compulsory dissolution of the business. The CCA applies to domestic legal entities and any foreign companies (incorporated or not) that have an office, branch, or representation in Brazil.

Since the enactment of the CCA, several agencies have issued regulations aiming to clarify and facilitate the implementation of the CCA's requirements.

1. March 2015 Decree

Although the CCA became effective in January 2014, in practice, enforcement was not enabled until over a year later, when (in March 2015) then-incumbent president Dilma Rousseff issued a decree regulating key aspects of the law (Decree No. 8420/2015). Among other things, the decree provided sentencing guidelines with a clear focus on prevention, specifically rewarding companies with a strong compliance program in place with a discount off the applicable fines.

To be considered effective and warrant a lesser fine, such a program must include the following elements: (i) an adequate tone at the top; (ii) written integrity policies (e.g., standards of conduct, code of ethics and anti-corruption procedures) applicable to all employees, members of management and, as appropriate, third parties; (iii) periodic compliance training; (iv) periodic risk assessments, with an aim to enhance and update the compliance program; (v) thorough and truthful bookkeeping; (vi) internal controls ensuring the accuracy of financial reports; (vii) specific procedures to prevent fraud and other misconduct in connection with public tenders, government contracts, and any interactions with public officials (e.g., paying taxes, handling inspections, or applying for licenses), including through third parties; (viii) a compliance function with adequate structure, independence, and powers to implement the integrity program; (ix) adequately publicized reporting mechanisms, which must be accessible to employees and third parties, as well as whistleblower protection measures; (x) disciplinary measures for misconduct; (xi) mechanisms ensuring detection, prompt discontinuation, and timely remediation of misconduct; (xii) due diligence for third parties (including suppliers, contractors, agents, and business partners); (xiii) due diligence, background checks and exposure assessments prior to any corporate reorganization (including mergers and acquisitions); (xiv) continuous monitoring of the compliance program, with an aim to improve internal controls and (xv) transparency in donations to candidates and political parties. When assessing a compliance program, the authorities must take into account the company's size and structural complexity, as well the use of third-party intermediaries, among other factors.

In addition to an effective compliance program, other mitigating factors include cooperating with the authorities, self-reporting misconduct, and remediating damages. Conversely, companies face fine increases when company management has knowledge of the wrongdoing and fails to prevent it, or when there is a pattern of continuous or recurrent offenses.

Furthermore, the decree also clarified the role of different agencies with overlapping powers to enforce the CCA. Civil sanctions must be pursued in court, through legal action initiated, as a rule, by the Office of the Federal Attorney-General ("AGU"). As for administrative penalties, generally, the government institution directly affected by an alleged offense has primary jurisdiction to conduct and judge the corresponding sanctions proceeding. However, within the Federal Executive branch, the Office of the Federal Comptroller-General ("CGU") has jurisdiction over the matter, *inter alia,* (i) where the entity primarily affected is unwilling or unable to do so, (ii) where multiple federal entities are affected; (iii) in complex or relevant cases; and (iv) in cases involving more than one body or entity of the federal public administration.

2. Regulations by the CGU

In the years following the March 2015 decree, to structure and govern its newly expanded sanctions regime, the CGU issued a series of additional regulations and guidelines. Most recently, the CGU issued Normative Instruction No. 13/2019, which sets out the proceedings for determining administrative liability of legal entities under the CCA (effectively revoking the contents of the previously applicable Ordinance No. 910/2015, which dealt with the same subject matter). Among other things, the Normative Instruction determines which government institutions are responsible for initiating and judging the administrative proceedings under the CCA; the Instruction also sets out detailed rules pertaining to the investigation of alleged misconduct.

Prior to this most recent guidance, the CGU had also issued a regulation (in 2015) dealing with the evaluation of compliance programs (CGU No. 909/2015). That regulation establishes a three-pronged test for companies to earn a fine reduction based on the implementation of an effective compliance program. Specifically, companies must demonstrate: (i) which of the controls in the March 2015 decree (described above) are included in the compliance program, and prove that they are adequate to the company's size, operations, and relevance in the market; (ii) that the program has been consistently and effectively implemented over time, including through written records, statistics, and sample case files; and (iii) that the program had been created prior to the alleged misconduct, and that it was used to prevent, detect, and remediate the specific acts under review. To satisfy such prongs, companies may submit evidence including official documents, emails, memoranda, minutes of meeting, reports, internal policies, and payment or accounting data.

In addition, to ensure greater uniformity in the evaluation of compliance programs by the different government institutions that have jurisdiction to conduct administrative proceedings under the CCA, the CGU released a "Practical Guide for the Evaluation of Compliance Programs" in September 2018. The Guide sets forth the requirements and methodology for the analysis and evaluation of a compliance program. More specifically, it classifies the 15 elements of an effective compliance program provided by the March 2015 Decree into three blocks (organizational culture of integrity; integrity mechanisms, policies and procedures; and the legal entity's actions in response to the illegal act) and provides over 100 specific questions in relation to these blocks. The Guide contains an Evaluation Spreadsheet that automatically calculates the percentage of reduction of the fine based on (yes/no/partially) answers to those questions. By way of example, the Evaluation Spreadsheet asks whether senior management and employees have received anti-corruption training over the previous 12 months; whether the company's compliance representative has a direct reporting line to the highest management level; whether the company conducted anti-corruption and anti-fraud risk assessments over the previous 24 months;

whether third-party due diligence includes a verification of past corruption cases and adoption of compliance programs; and whether the company took appropriate disciplinary action against those implicated in illegal acts.

3. New Guidelines on Corporate Settlements under the CCA

Among other innovations, the CCA created anti-corruption “leniency agreements,” under which companies that effectively cooperate with the investigations and the administrative proceedings may avoid debarment sanctions and reduce administrative monetary fines by up to two-thirds. To be eligible for such benefits, companies must immediately cease any participation in the corrupt conduct, admit to the wrongdoing, and cooperate fully and permanently with the investigation. While the law detailed the requirements and benefits of such settlements, it failed to provide sufficient guidance on the negotiation process. This caused uncertainty among different agencies with anti-corruption responsibilities, arguably hampering enforcement.

Several agencies have taken steps to address this gap and better define and coordinate their respective roles, as well as the procedural rules for reaching leniency agreements. These agencies include (i) the CGU; (ii) the AGU; (iii) the Federal Public Prosecutor’s Office (MPF); and (iv) the Federal Court of Accounts (“TCU”), which has powers to enforce certain administrative sanctions and also audit and suspend (where applicable) government acts involving federal entities or funds.

Most recently, the CGU and the AGU published a joint regulation in August 2019, which details the leniency agreement procedures, and provides guidelines for cooperation between the two agencies with a view to increasing transparency and optimizing their performance in conducting the agreements established on the CCA. Pursuant to the regulation, members of both agencies shall be part of the commission tasked with negotiating leniency agreements, and shall jointly decide whether to execute the agreement. Additionally, CGU and AGU implemented Normative Instruction No. 2/2018, which provides the methodology to calculate administrative fines in leniency agreements under the CCA. The disclosed goal was to expand the transparency and consistency of the application of fines.

While the precise role of each agency may continue to evolve, these developments suggest that the authorities will increasingly join efforts to negotiate leniency agreements. For instance, in June 2019, the CGU, the AGU and the MPF, along with the U.S. Department of Justice (“DOJ”), executed the TechnipFMC plc leniency agreement, the first leniency agreement deriving from a multilateral and joint investigation in connection with Operation Car Wash. As of September 2019, twenty-seven leniency agreements have been entered in Brazil (eighteen with the MPF and nine with CGU/AGU).

4. Brazilian Central Bank and Securities and Exchange Commission (CVM) regulations on corporate settlements

Since 2017 (following enactment of Law No. 13/506), the Brazilian Central Bank and the Securities and Exchange Commission of Brazil (CVM) can also enter into corporate settlements (dubbed “Administrative Settlement in Supervisory Proceedings”), similar to the leniency agreement provided for in the CCA. Under the corporate settlement regime, cooperating companies may receive full immunity or a two-thirds reduction of the administrative monetary fine. To be eligible for such benefits, companies must immediately cease any participation in the corrupt conduct, admit to the wrongdoing, and cooperate fully and permanently with the investigation. In addition, these benefits are only available if Central Bank or the CVM does not hold sufficient evidence to ensure conviction of the cooperating individuals or legal entities at the time of the proposal of the agreement. These corporate settlements (which are administrative in nature) do not prevent the MPF from opening criminal proceedings against the collaborating legal entities or individuals. Both the Brazilian Central

Bank and the CVM recently issued additional regulations (Regulation BACEN 3,857/2017 and Instruction CVM No. 607/2019), further detailing, *inter alia,* procedural rules for negotiating and executing administrative settlements, and the benefits that may be provided to cooperating individuals and legal entities.

II. China

The sweeping momentum of China's anti-corruption campaign continued in 2019. During the first half of the year, the Supervision Commissions of various levels in China received approximately 1.61 million complaints and whistleblowing letters, opened 315,000 cases, and punished more than 250,000 officials for violations of the Communist Party of China's ("CPC" or the "Party") disciplinary regulations. Eleven high-level central government officials were investigated for corruption in 2019, including the former CEO of CITIC Group, Vice Director of China Tobacco, and former Vice Governor of Sichuan Province. Chinese state media has specifically noted that an increasing number of officials, including two central government officials, turned themselves in to relevant authorities in 2019—a sign that officials are beginning to understand the sweeping and relentless nature of the anti-corruption campaign.

The "Sky Net" Operation, China's multi-organ-effort to capture Chinese fugitive suspects that fled aboard, also shows no signs of slowing down. In the first three months of 2019, a total of 374 fugitives were detained and returned to China, recovering assets of over RMB 627 million (approximately $88.7 million). Since the initiation of the "Sky Net" Operation in May 2014, China has recovered around RMB 14.25 billion (approximately $2.02 billion) and repatriated more than 5,900 fugitives, including 58 of the 100 most-wanted corrupt Chinese fugitives.

Other recent anti-corruption developments suggest that China's efforts are not just limited to investigating and punishing corrupt officials. Rather, efforts in the private sector to prevent and punish corruption of company employees, the focus on integrity for the Belt-and-Road Initiative, the launch of China's corporate social credit system, and the anti-corruption campaign in the healthcare industry all signal an intent to create a cleaner business environment.

Finally, China's newly adopted Internal Criminal Judicial Assistance ("ICJA") law has the potential to impact both domestic and foreign anti-corruption investigations.

A. The Rise of Anti-Corruption Efforts in the Private Sector

While the anti-corruption campaign has maintained focus on government agencies and SOEs, an increasing number of private Chinese companies have joined the battle to fight "internal" corruption (i.e., corruption of their own employees). In January 2019, Agile Property, a prominent real estate developer in China, issued a notice that it had terminated a regional vice president for allegedly accepting high value bribes. Also in January, DJI Technology, a Chinese drone manufacturer, announced that an audit had revealed that widespread corruption in its supply chain cost the company more than $140 million in 2018. Forty-five employees were identified and disciplined for having allegedly been involved in the scheme. In September 2019, property conglomerate Dalian Wanda revealed that it had terminated four managers for soliciting and accepting millions of dollars in bribes; the four individuals were handled to judicial organs for criminal investigations.

Many large Chinese companies have granted their internal audit departments greater power in detecting and investigating fraud and corruption. Alibaba has established an Integrity Compliance Department, responsible for conducting internal investigations against violations of company policies. The Ethics Committee at Baidu is responsible for investigating corruption-related issues. It operates independently from other departments and reports directly to the Baidu's top management. Dalian Wanda's internal audit department is the only department that is directly managed by its Chairman to ensure that it maintains necessary independence and support.

Private companies are also taking steps to encourage whistleblowers, a notoriously difficult task for Chinese companies. For example, JD.com, a giant B2C online retailer in China, has set up a RMB 10 million (approximately $1.3 million) fund to provide financial rewards to whistleblowers.

Currently, there are two social organizations in China formed by private companies with the goal to tackle fraud and corruption: the Anti-Fraud Alliance and the Trust and Integrity Enterprise Alliance. All the member companies of these organizations have vowed zero tolerance towards corruption and agreed to work together toward this common goal. One of the mechanisms to achieve this goal is a shared “blacklist.” The organizations maintain databases with information on corrupt vendors and individuals. Any party in the databases will be blacklisted by all the member companies.

While the corruption cases disclosed by private companies show that corruption issues are being treated more seriously than in the past, China still has a long way to go. To date, these efforts have been limited to large Chinese enterprises. China has around 27 million private companies, many of which are small or medium size. There is no evidence that these companies are taking any steps toward anti-corruption compliance. Moreover, while the focus of reducing internal corruption is noble—and notable for those foreign companies serving as suppliers and business partners with these large private Chinese companies—there still appears to be limited attention given to reducing external corruption (i.e., bribery and corrupt acts of their employees aimed at external parties) within these companies.

B. Compliance Focus of Belt and Road Initiative

China’s Belt and Road Initiative (“BRI”) is an infrastructure investment program that connects Asia with Africa and Europe through land and maritime networks. There are more than 70 economies geographically located along BRI transport corridors, and the projects within the BRI are designed to increase trade, improve regional integration, and stimulate economic growth among the corridor economies.

Thus far, 131 countries and 30 international organizations have joined the BRI. By some estimates, the total budget for the BRI is around $1 trillion. As the scale of the BRI has expanded, concerns and criticisms have followed. Some view China’s loans to financially stressed nations as debt traps that will allow China to exert more political influence, and the lack of standards and transparency in procurement can easily fuel corruption, especially in some of the BRI corridor countries where corruption is endemic. In response, China has signaled that it plans to increase transparency and seek more international cooperation.

At a high profile Belt and Road Forum in April 2019, President Xi stated that BRI projects will be of “higher quality” and that all the operations will be “exposed under the sun,” vowing zero tolerance for corruption. The concept of “Clean Belt and Road” was first brought forward by President Xi in 2017. Since then, China has taken several steps to alleviate BRI related corruption risks, such as controls on Chinese SOEs and increased involvement of the Central Commission for Discipline Inspection (“CCDI”) in BRI projects.

1. Controls on SOEs

Chinese SOEs have been central figures in the BRI. According to China’s State-owned Assets Supervision and Administration (“SASAC”), as of October 2018, central SOEs had participated in more than 3,000 projects. Among the BRI projects started and scheduled, around 50% involve central SOEs.

Around the end of 2018, SASAC issued *Central SOEs Compliance Management Guidelines (Trail)*. Shortly thereafter, the National Development and Reform Commission and other government agencies issued a

Corporate Management Guideline for Compliance Overseas. The two guidelines provide guidance in areas such as the structure of compliance programs, risk assessments, compliance program implementation, and compliance culture cultivation, and encourage Chinese companies to increase audits and controls over overseas operations and personnel. In SASAC's first internal journal in 2019, it called 2019 the year of "improving central SOE's compliance and risk controls" and said that one of its focuses in 2019 is to ensure that central SOEs are fully implementing the *Central SOEs Compliance Management Guidelines (Trail).* In addition, China, in coordination with outside groups such as the World Bank, has been organizing an increasing number of compliance trainings for SOEs to understand international best practices in terms of anti-corruption compliance.

2. CCDI Involvement

CCDI has been a key player in China's anti-corruption campaign. However, as has been widely reported, CCDI's efforts thus far have focused on domestic corruption. CCDI, and the Chinese government more broadly, have shown little appetite to tackle the issue of Chinese companies, especially Chinese SOEs, acting corruptly while operating abroad. This is a primary concern in connection with the BRI.

CCDI has been seeking strategies to alleviate some of these concerns. In particular, CCDI has been looking for ways to cooperate with authorities in BRI countries to monitor the projects and the Chinese companies working on them. For example, the CCDI formed a joint inspection team with authorities from Laos to supervise the construction of the China-Laos Railway, a project valued around $5.2 billion. CCDI dispatched its inspectors to work together with contractors and has met regularly with authorities from Laos to exchange information and tackle potential corruption issues. Thus far, the China-Laos Railway project has closed 22 tenders ($2.58 billion). According to reports, all of the tenders have been vetted for signs of misconduct including corruption, bid rigging, and unauthorized disclosure of confidential information. While such steps are important, it remains to be seen whether the Chinese government, through CCDI or otherwise, is willing to punish SOEs or their employees for corruption of foreign government officials.

C. Corporate Social Credit System

In another effort, China has begun implementing a social credit system ("SCS") to rate companies and individuals on a variety of factors (compliance with corruption laws, tax regulations, environmental standards, etc.) and to apply rewards to individuals and companies with high ratings and sanctions to individuals and companies with low ratings.

Originally announced in 2014, the SCS relies on metadata and technology to monitor and guide behavior of individuals and companies through individual and company ratings. While the two parts can impact each other (e.g. an "untrustworthy" individual may not be allowed to take the position as a legal representative, director, supervisor, or senior executive in a company; the legal representative of a company deemed "untrustworthy" could be forbidden from air travel), each has its own mechanism, rating requirement, and state actors involved. The SCS rating system for corporations has advanced much farther than the rating system for individuals, and its development accelerated in 2019, with China issuing a number of documents guiding the process and regulating the details of corporate SCS.

Corporate SCS uses the data collected through companies, government inspections, and other sources to assess the performance of companies against a vast number of government-issued requirements (around 300 for a multi-national company and less for a company with smaller operations) in the form of different categories of rating. The corporate ratings will be algorithm-based, applying different weight to different requirements according to relevant regulations, and the ratings will cover a broad spectrum including tax, customs authentication, environmental protection, product quality, work safety, e-commerce and cybersecurity. Companies with good ratings can enjoy

preferential treatments such as faster administrative approval processes and easier access to commercial loans. Conversely, companies with low ratings could be deemed untrustworthy. An untrustworthy company can be jointly sanctioned by various government authorities. While the sanctioning systems are not fully implemented at this stage, a major goal of such sanctions is to punish companies in essentially every aspect of business in China, forcing the companies to comply with Chinese laws and regulations.

Under the joint sanctions approach, a violation in one area can create significant hurdles for the company to conduct business. For example, small commercial bribery (less than approximately $8,400) in China is usually regulated by the Market Regulation Authorities and typically can be resolved with a fine. However, once the joint sanctions are implemented, a company that commits commercial bribery could face multiple sanctions from government agencies who have no oversight on commercial bribery – the company may experience longer customs clearance periods, more inspections from various government agencies, and fewer tax benefits. Given the potential severe consequences of a simple deviation from Chinese laws and regulations, corporate SCS pushes companies operating in China, domestic and foreign, to take a proactive approach toward understanding the requirements applicable to them and taking necessary steps to address any deficiencies.

Critically, it appears that a company's ratings can be affected by the conduct of its business partners, which demands a company monitor its third parties for their ratings and trustworthiness until the relationships end. Moreover, because individual ratings have impact on corporations, the corporate SCS arguably makes it necessary for companies to vet senior managers. Both aspects—third party monitoring and employee screening—should be familiar to companies with a robust compliance system but could place a heavy burden on small and medium-sized enterprises with less developed compliance programs.

Although the corporate SCS will increase the compliance cost of doing business in China, it may help level the playing field for foreign companies. It is not a secret that government authorities in China have great discretion in deciding how to interpret and enforce certain laws. Such uncertainty can turn into business opportunities, the benefit of which has typically been enjoyed by local companies, which usually have a better relationship with authorities than their foreign competitors. In theory, the automated regulatory system of the SCS could create a more level playing field.

D. Anti-Corruption Campaign in the Healthcare Sector

The healthcare sector in China has long been plagued by corruption. One need look no farther than the number of high-profile FCPA resolutions that have involved China's healthcare industry (see, e.g., Fresenius (2019), Stryker (2018), GSK (2016), SciClone Pharmaceuticals (2016), Novartis (2016), AstraZeneca (2016)). It is estimated that around 30% of the cost of drugs in China goes to doctors' pockets as kickbacks for prescriptions.

A cleaner healthcare sector appears to be a focus of healthcare regulators in 2019. At China's January 2019 National Health Conference, relevant authorities stressed the importance of eliminating corruption in public hospitals. In May 2019, the National Health Commission held a meeting focusing on Party compliance and anti-bribery, signaling more incoming probes into public hospitals and state-owned medicine and medical device manufacturers. Also in May, nine government agencies, including the Finance Ministry, the Ministry of Commerce, the Ministry of Public Security, and the National Health Commission, issued a notice of major focus areas in 2019 in the healthcare industry. Among the key points was cracking down on commercial bribery in the healthcare industry.

In the first eight months of 2019, at least 12 directors of public hospitals have been investigated or arrested for corruption in China. Fourteen types of drugs and their manufacturers are banned from participating in public

procurement in Hunan province due to alleged kickbacks. Over 30 publicly-traded pharmaceutical companies in China received inquiries from the Shanghai Stock Exchange and Shenzhen Stock Exchange regarding their 2018 annual reports, with a focus on sales expenses. More than 70 pharmaceutical companies in China are being audited by the Ministry of Finance working jointly with relevant health insurance bureaus. The Medical Associate of Yunnan Province has announced that it will no longer accept any donations related to trainings and conferences from medicine or medical device manufactures or their distributors.

Pharmaceutical companies found paying improper benefits to doctors are facing more serious penalties. For example, in Jiangsu province, a pharmaceutical company that committed bribery will be forbidden from supplying drugs, equipment or medical supplies anywhere in the province for two years, and all on-going contracts will be terminated. Penalties for doctors taking bribes are equally severe. In Shanghai, doctors who accept improper benefits (including cash, gift cards, vouchers, reimbursement of personal expenses, entertainment, and kickbacks) of more than RMB 5,000, accepted bribes of any value more than once, or solicited bribes, will be dismissed, and their licenses to practice will be revoked. With corporate SCS and individual SCS around the corner, the penalties for pharmaceutical companies and doctors who cross this red line will only be magnified.

E. Criminal Judicial Assistance Law

On October 26, 2018, the ICJA was passed in the legislature of the People's Republic of China. The ICJA creates rules and restrictions related to China's cooperation with foreign authorities in connection with criminal investigations and prosecutions. The ICJA is intended to fill the gap for countries where China does not have mutual legal assistance treaty ("MLAT") and provide domestic law to clarify the roles and responsibilities of relevant government agencies in the process of providing or requesting judicial assistance, whether an MLAT is in place or not.

The ICJA governs all incoming and outgoing requests for "criminal judicial assistance," including service of documents, investigation and document collection, witness interviews or testimony, seizure, detention, and freezing of assets, confiscation and return of proceeds of criminal activity, and transfer of convicted persons. ICJA creates a two-level review of requests for judicial assistance and authorities at both levels are given broad discretion to review these requests. Article 14 of the ICJA provides enumerated circumstances under which a request for assistance may be denied, including when: (i) the crime about which the request is made is political in nature or is a military offense; (ii) the act under investigation is not a crime in China; (iii) the crime has already been investigated or is under investigation or prosecution in China; (iv) the request for assistance is to further an investigation or prosecution based on race, religion nationality, gender or political opinion; or (v) there is no connection between the requested assistance and the matter at issue. Moreover, Article 14 includes a catch-all justification for denying a request, essentially allowing the Chinese authorities to deny a request whenever they deem it appropriate.[36]

Article 4 of the ICJA is particularly noteworthy for foreign investigators as well as Chinese companies and multinationals operating in China. The first part of Article 4 prohibits a foreign authority from conducting criminal proceedings (including evidence gathering and witness testimony) in China without the proper approvals. The second part of Article 4 restricts companies (including apparently Chinese subsidiaries or branches of multinational companies) and individuals from providing evidence located in China to foreign criminal investigators unless the foreign regulator first obtains proper approval from the Chinese authorities. As a result, a multinational corporation may be prevented from cooperating with a foreign investigator unless and until that foreign investigator obtains the necessary approval from the Chinese authorities. This *could* create a myriad

36. Article 14 of the ICJA, *available at*: http://en.pkulaw.cn/display.aspx?cgid=b1575aa60196ebe4bdfb&lib=law

complications for a multinational company attempting to navigate a foreign corruption investigation related to conduct in China.

It remains to be seen how this provision will be applied. China has yet to issue guidance on the ICJA and a history of its application in practice has yet to be established. However, foreign regulators and companies and operating in China should be alert and plan for its potential application to a foreign criminal corruption investigation involving evidence in China.

III. <u>Mexico</u>

A 2015 constitutional reform has led to a complete revamping of Mexico's anti-corruption system over the past few years and a renewed interest and vigor in Mexico's fight against corruption. While significant work remains, Mexico appears positioned to greatly increase its anti-corruption efforts, changing the landscape for both Mexican officials and domestic and foreign companies and individuals operating in Mexico. To appropriately understand the new anticorruption system (the National Anticorruption System, ("NAS")) and the current state of Mexico's anti-corruption efforts, this section covers (i) a description of the former anticorruption system; (ii) the key features of the NAS; and (iii) a perspective of how the NAS has been implemented so far.

A. Former Anticorruption System

Prior to the adoption of the NAS, the anticorruption framework in Mexico was not specialized and was mostly contained in criminal codes. For example, the Federal Criminal Code criminalized conduct committed by public officials such as the improper exercise of public service, abuse of power, embezzlement of public funds, intimidation, influence peddling, active and passive bribery, and foreign bribery. Therefore, the federal and state Attorney General's offices, which were not specialized in anticorruption, mostly performed the anticorruption enforcement in the former system. After the federal or state prosecutors charged an individual or a corporation with a corruption-related offense, the criminal courts (which were not specialized in anticorruption) decided the fate of the charged.

From an administrative perspective, there were other federal laws that addressed anticorruption, but with a much narrower scope. For example, the Federal Anticorruption Law on Public Procurement was limited to corruption in the federal procurement context. Nevertheless, under these laws, public officials could be terminated and fined for corruption. Similarly, private parties could be banned from participating in public bids, fined or even dissolved (if a corporation). The public institution that was in charge of investigating and adjudicating these administrative penalties was the Ministry of the Public Function (Secretaría de la Función Pública), more broadly defined as in charge of monitoring the conduct of public officials, including their interaction with private parties, and sanctioning its deviations.

In the former anticorruption system, no institution was endowed with an effective coordination mission between federal and state governments.

B. The National Anticorruption System

1. Context

Despite being the second largest economy in Latin America, corruption is still pervasive and represents a significant risk for companies operating in Mexico. International organizations have recognized this problem and highlighted the evolution of the Mexican legal framework as an imperative necessity. As the current OECD's

Secretary General, Miguel Ángel Gurría, affirmed, the adoption of the NAS responded to a problem that has plagued the country for far too long. According to the 2017 Transparency International Corruption Perceptions Index, Mexico was ranked 125th out of 180 countries, moving down in 2018 to the 138th position (ranking below Laos, Honduras and Sierra Leone). Mexico's National Statistics Office (INEGI) informed that corruption is considered one of the main concerns of Mexican citizens.

In an era where various other countries in the region were modernizing their anticorruption systems, Mexico could not fall behind. For example, Brazil modernized its anticorruption framework in 2013 with the enactment of the Clean Companies Act (Law No. 12846/13). Argentina made the same with its anticorruption framework, which evolved recently and is now based in the Argentinian Criminal Code and the recently enacted Law n° 27.401, published in the Official Gazette on December 1st, 2017.

2. Legal Framework

On May 2015, Mexico amended its constitution to create the NAS. The NAS provides for the enactment and amendment of several laws. The enacted laws include the General Law of the NAS ("NAS Law"), the Federal Tribunal's Administrative Justice Organizational Law ("Administrative Justice Law"), the General Administrative Responsibilities Law ("Administrative Responsibilities Law") and the Federal Audit and Accountability Law ("Audit and Accountability Law"). Other existing laws were amended to support and align with the NAS, including the Federal Criminal Code, the Federal Public Administration Organizational Law and the Federal Attorney General's Office Organizational Law. Both enactments and amendments have been acknowledged by the OECD as important steps forward in the fight against corruption, however, their implementation still shows a bleak picture.

3. Understanding the New Mexican Approach

Mexico's new approach to fighting corruption involves the creation of several new institutions specialized in anticorruption, the effective coordination between federal and state governments, the participation of the civil society in the development of policies and coordination efforts, and the adoption of essential anticorruption features (such as corporate administrative liability, consideration of compliance programs, transparency into the assets of public officials, among others).

a. New Institutions

A key focus of the NAS is to create new institutions specialized in anticorruption. However, the involvement of the civil society in the fight against corruption and its coordination with the authorities is probably the most notable feature of the NAS. The NAS seeks to coordinate private citizens and authorities from different scopes of government in order to improve the prevention, investigation and sanctioning of corruption.

The following are the new institutions created by the NAS:

Anticorruption Prosecutor's Office. The Anticorruption Prosecutor's Office is a specialized office tasked with the investigation and charging of corruption-related offenses. Critically, the Anticorruption Prosecutor's Office will maintain independence through its (1) special appointment and removal processes, autonomy in the exercise of human, material and budgetary resources, and autonomy in the investigation of cases, among other things. The head of the Anticorruption Prosecutor's Office is the Special Anticorruption Prosecutor. The first Special Anticorruption Prosecutor was appointed by two thirds of the Senate's votes for an unrestricted term, thereafter it will be appointed by the National Attorney General.

Specialized Administrative Judges. These judges adjudicate administrative sanctions to public officials and private parties involved in corruption. Specialized Administrative Judges belong to the Federal Tribunal of Administrative Justice, which is tasked with their appointment: three within its Superior Chamber (its highest court) and 15 distributed among its Regional Tribunals (highest regional federal administrative courts.

Coordinating Committee. The Coordinating Committee is in charge of the development of national anticorruption policies, coordination between institutions, monitoring and progress evaluation. It is composed of the heads of the Ministry of the Public Function, the Federation's Superior Audit Committee, the Federal Tribunal of Administrative Justice, the Anticorruption Prosecutor's Office, the National Institute for Transparency, Access to Information and Protection of Personal Data, the Federal Judicial Council and the Citizens' Participation Committee.

Citizens' Participation Committee. The Citizen's Participation Committee is entrusted with a consulting mission by means of opinions and proposals for the development of anticorruption national policies. Through the participation of its head in the Coordinating Committee it is also involved in the coordination, monitoring and evaluation of the NAS. Five prestigious citizens with contributions towards transparency, accountability, or the battle against corruption form the committee.

Governing Committee. The Governing Committee is responsible for (1) designing, approving and promoting comprehensive policies on oversight; (2) implementing the coordination mechanisms among all members of the NAS; and (3) implementing the system for information exchange regarding the control of public resources. The Governing Committee is formed by the Federation's Superior Audit Committee, the Ministry of the Public Function and seven rotating members from the states' anticorruption systems.

Local anticorruption systems. As part of the NAS, states are required to establish their own respective local anticorruption systems, which are to have full coordination with the federal institutions for the prevention, detection, investigation and sanction of corruption.

b. Renewed Organization

With the adoption of the NAS, corruption is still mainly dealt with from a criminal perspective, yet with a more specialized focus and robust process. However, there is a new emphasis in the administrative realm.

From the criminal perspective, corruption-related offenses are now investigated and prosecuted by a specialized office before being judged by the criminal courts.

From the administrative perspective, the Administrative Responsibilities Law establishes two different sanctioning procedures depending on the severity of the alleged offence: serious and less serious offences. For less serious offences, internal control bodies within the different government entities are responsible for investigating offences and imposing relevant sanctions. For serious offences, the Federal Tribunal of Administrative Justice is not limited anymore to deciding just on the legality of administrative or tax laws and acts of the federal government, but is also entrusted with deciding cases related to serious corruption offences, through its specialized administrative judges.

Furthermore, within the legislative branch, the Federation's Superior Audit Committee is tasked with reviewing and auditing the federal government's spending and to inform the Anticorruption Prosecutor and the Federal Tribunal of Administrative Justice of any findings of corrupt practices.

The NAS contemplates the coordination of federal, local and municipal scopes of government, a mission that is entrusted to its Coordinating Committee.

c. Key Features of the NAS

The NAS has several features, some of them completely new to the Mexican legal system, which puts it along the most modern anticorruption systems in the world. The most relevant are:

Corporate Criminal Liability. Article 11 of the Federal Criminal Code establishes the possibility for the judge to decide the suspension or dissolution of a corporation, as well as economic penalties, for acts committed by any member or representative in a crime committed in the name or under the protection of or for the benefit of the corporation. Furthermore, Article 222 of the same code indicates the range for economic penalties applicable to the violations in Article 11, and provides for an adjustment of the economic penalty depending on the degree of knowledge the administrative bodies had, the damage caused, as well as the benefit obtained by the corporation.

Corporate Administrative Liability. Article 24 of the Administrative Responsibilities Law provides for the sanction of corporations for acts related to serious administrative faults, including corruption committed by individuals acting on behalf or in representation of the corporations and seeking to obtain benefits for the corporation.

Anticorruption Compliance Programs. Article 25 of the Administrative Responsibilities Law states that the existence of an “integrity policy” within the legal entity will have to be assessed as part of the determination of a corporation’s liability and enumerates the minimum elements that such policy must contain.

Under Article 25 of the Administrative Responsibilities Law, compliance programs must contain the following elements: (i) an exhaustive organization and procedures manual; (ii) a code of conduct; (iii) adequate and effective control, monitoring, and auditing systems; (iv) adequate alert mechanisms and disciplinary processes; (v) appropriate training systems and processes; (vi) human resources policies aiming at avoiding the incorporation of people who can generate a risk to the integrity of the corporation; and (vii) mechanisms that guarantee the transparency and publicity of the corporation’s interests at all times.

The establishment of appropriate compliance programs are to be considered as a mitigation factor by authorities while deciding on the corporation’s sanctions. On June 2017, the Ministry of the Public Function presented a model program for corporate integrity as guidelines for corporations.

Foreign Bribery. The Federal Criminal Code prohibits Mexican companies and individuals from bribing foreign government officials. It does not cover commercial bribery.

Disclosure of assets and tax returns for public officials. Article 32 of the Administrative Responsibilities Law requires public officials to disclose their assets and taxes, and declare conflicts of interests.

Active Bribery. Under Article 222 of the Federal Criminal Code, it is a crime to commit active bribery, punishable by imprisonment from 3 months to 14 years and economic penalties from MXN 2,500 to 8,500, depending on the amount of the bribe.

From the administrative perspective, Article 66 of the Administrative Responsibilities Law forbids the active corruption of public officials by private persons. Pursuant to article 81, three types of sanctions can apply to corporations for such misconduct : (i) economic sanctions that may reach up to two times the benefits obtained or, in the case of not having obtained them, for the amount of MXN 8,500 to 12 million; (ii) a temporary

disqualification from participating in public bids for a period no less than three months and no longer than eight years; and (iii) compensation for the damages caused.

Passive Bribery. Pursuant to Article 222 of the Federal Criminal Code, passive bribery is committed when a public official, either personally or through an intermediary, *requests or receives* money or any other gift for himself or any other party, or accepts a promise, to perform or fail to perform any legal or illegal act in relation to his functions. The same article contains a special provision for misconduct of the federal legislator, which in the exercise of its functions, and within the framework of the approval process of the respective expenditure budget, request the allocation of resources in favor of a public entity in exchange of an undue advantage.

From the administrative perspective, such misconduct is prohibited by Article 52 of the Administrative Responsibilities Law. Pursuant to Articles 78 and 79 of the Administrative Responsibilities Law the sanctions are: (i) the suspension or dismissal from employment, office, or commission for a maximum period of 90 days; (ii) economic sanctions that must not exceed twice the amount of the profit generated by the offender, without being less than or equal to such profit; and (iii) the temporary disqualification from holding public service jobs, positions or commissions and participation in acquisitions, leases, services or public works, for a period ranging from three months (if no profit was generated) to 20 years.

Facilitation Payments. Defined as payments "made to secure or expedite the performance of a routine or necessary action to which the payer has legal or other entitlement," facilitation payments are prohibited.

Gifts and Entertainment. Although it was formerly tolerated, government officials are no longer allowed to accept gifts or similar benefits "from any person or organization." As it stands, there is no exception to this rule, since the Administrative Responsibilities Law does not refer to other forms of hospitality such as meals, entertainment and travel.

Use of Intermediaries. Article 66 of the Administrative Responsibilities Law sanctions the corruption of public servants by private persons, whether the bribery act is committed directly or through third parties. Similarly, Article 222 of the Federal Criminal Code sanctions the direct or indirect passive bribery of a federal legislator.

C. Implementation of the NAS

To date, the implementation of the NAS has been mixed. While the major institutions have been created and certain high-profile positions have been filled, many positions remain unfilled. Moreover, there is no evidence to date that the new framework and infrastructure created by the NAS is being utilized in major corruption investigations.

1. Appointments

On February 2019, María de la Luz Mijangos Borja was appointed its Chief Anticorruption Prosecutor. However, many other key posts have not yet been filled. In particular, the 18 anticorruption judges of the Federal Tribunal of Administrative Justice that are to be appointed as per the NAS. After the Citizens' Participation Committee obtained a favorable ruling in their lawsuit filed against omissions by the executive branch and the Senate in the appointment of these 18 anticorruption judges, the Senate rejected the list that then-President Enrique Peña Nieto had sent. On a press release dated August 25, 2019, the Citizens' Participation Committee urged President Lopez Obrador to send a new list of candidates for ratification as soon as possible. President Lopez Obrador has not done so as of this date.

The appointment of these anticorruption judges is fundamental for the proper functioning of the NAS, since only they are responsible for the substantiation of procedures for serious administrative misconduct committed by public officials and by individuals involved in acts related to corruption.

2. Enforcement

Despite its strengthened legal framework, new specialized institutions and appointments, Mexico is yet to show the full potential of the NAS. The failure to appoint anticorruption judges has made it impossible to try cases for serious administrative misconduct. Also, the lack of public information on the prosecution of corruption cases makes it hard to understand the extent in which the NAS is being used. There have been some efforts to fight notorious corruption cases, but either these efforts have not gone through the NAS or results of ongoing investigations have proved slow and remain to be seen.

Most notably, Mexico's recent efforts to punish those companies and individuals involved in widespread corruption by Odebrecht have been handled outside of the NAS framework. As a result of Operation Car Wash in Brazil, Odebrecht's global corruption scandal became public on 2014. The first signs of the consequences in Latin America appeared on December 21, 2016, when the United States DOJ revealed documents regarding Odebrecht operation in Latin America, including bribes of more than $10 million in Mexico.

In 2017, Mexico's Ministry of the Public Function announced that it had identified "irregularities" between Pemex and Oderecht amounting to $6.7 million. In April 2018, Odebrecht was fined MXP 543 million (~$28 million) by the Mexican authorities, who also banned Odebrecht from contracting with the federal government, including Pemex, for a period of three years. These sanctions were issued in the wake of investigations that found that the business relationships between Odebrecht and Pemex were stained by corrupt practices.

Accusations subsequently surrounded Emilio Lozoya, a former CEO of Pemex for allegedly receiving $10 million in bribes from a former executive at Odebrecht in exchange for a contract related to Mexico's Tula refinery. On July 5, 2019, a Mexican judge issued a warrant for the arrest of Emilio Lozoya, his wife, mother and sisters, for their alleged involvement in the Odebrecht corruption scandal in Mexico. Charges against Emilio Lozoya include bribery and tax fraud.

The investigation conducted by the Mexican authorities into the Odebrecht case was not done by the Anticorruption Prosecutor's Office. Instead, it was the National Prosecutor's Office and the Unit of Financial Intelligence within the Ministry of Finance (Unidad de Inteligencia Financiera de la Secretaría de Hacienda y Crédito Publico), which shows that Mexico is not using the NAS to pursue this case.

Chapter 6: Multilateral Development Banks

Companies working in the area of infrastructure development *have to be aware* of the growing role MDBs play in the global fight against corruption and fraud. Chapter 6 provides an overview.

I. <u>Context</u>

The role played by multilateral development banks ("MDBs") in the global fight against corruption is now well-established. Sanctions by MDBs are powerful deterrents that have an impact not only on companies' eligibility for MDB-funded projects, but have far reaching reputational and business consequences. Preventative efforts by MDBs to encourage and require compliance programs are also beginning to have an impact, particularly for companies in Asia, Africa, and Latin America that may not have previously considered the need for anti-corruption compliance controls. Perhaps most importantly, MDBs can exercise "jurisdiction" over companies and individuals of any nationality and in any location, so long as an MDB-funded project in involved. As result, for companies from countries without strong foreign anti-corruption laws operating in countries without strong anti-corruption frameworks (such as Africa, Southeast Asia, and other parts of the developing world), MDBs present the primary enforcement threat.

Over the past two years, several large and prominent companies have been subject to sanctions by MDBs for various forms of misconduct, including divisions of General Electric, Merck & Co., and Odebrecht and several of the largest Chinese construction companies. However, these represent just a fraction of the total enforcement activity by MDBs, which often include smaller engineering, consulting, or construction firms, "local" rather than international companies, and other entities that may be less sophisticated in the area of anti-corruption compliance.

II. <u>Overview of MDB Sanctions Regimes</u>

A. World Bank Sanctions Regime

The World Bank's current sanctions regime is set out in full in the "Bank Procedure: Sanctions Proceedings and Settlements in Bank Financed Projects," issued on June 28, 2016, with an effective date of January 7, 2016 ("Sanctions Procedures").

1. Investigation and Adjudication: Main Actors and Process

The core of the World Bank's sanctions regime is built around three main actors: the Integrity Vice Presidency, the Office of Suspension & Debarment and the Sanctions Board, which respectively represent the Bank's investigatory branch and two adjudicatory bodies.

Integrity Vice Presidency: The Integrity Vice Presidency ("INT") is primarily responsible for investigating allegations of sanctionable practices on Bank-funded projects. INT learns of potential violations through various sources, including government officials of the borrowing country (e.g., members of the implementation agency or the bid evaluation committee), World Bank staff participating in the project, local or international press and whistleblowers (e.g., competitors). Typically, once INT has concluded its investigation and finds that there is sufficient evidence supporting the allegations of sanctionable practices, INT summarizes its findings in a Statement of Accusations and Evidence ("SAE") and refers the case to the Office of Suspension & Debarment for first-level adjudication.

Office of Suspension & Debarment: The Office of Suspension & Debarment ("OSD"), headed by the Suspension and Debarment Officer ("SDO"), acts as the initial (and, often final) adjudicator of cases brought by INT. The OSD determines if the evidence supports a finding of a sanctionable practice under the applicable World Bank Procurement, Consultant or Anti-Corruption Guidelines and, if so, may recommend the imposition of sanctions by issuing a "Notice of Sanctions Proceedings" to the respondent. If the respondent does not contest

the OSD's recommended sanctions, the sanctions are imposed as recommended and the OSD's decision is published on the OSD's website. If the respondent wishes to contest the recommended sanctions, the respondent can do so through two non-exclusive options. The respondent may, within 30 days of receipt of the Notice, submit a written "Explanation" to the SDO, who, upon review of the Explanation, may (i) maintain the initial recommendation, (ii) revise the recommended sanctions or (iii) withdraw the Notice. The respondent can then appeal the SDO's decision to the Sanctions Board. The respondent can also choose to bypass the SDO and file a written "Response" directly with the Sanctions Board within 90 days of its receipt of the Notice. During fiscal year 2018, more than half of all sanctions cases (57%) were resolved at the OSD level and only 20 firms and individuals were sanctioned at the Sanctions Board level.

Sanctions Board**:** The Sanctions Board is the final adjudicator of contested cases and is the first non-Bank affiliated body to review each sanctions case. Unlike the OSD, which is composed entirely of World Bank-appointed staff, since 2016 the Sanctions Board has consisted of five members and two alternates, all of whom are external to the World Bank and who may not hold any appointment within the World Bank, IFC, or MIGA. Prior to the 2016 revision of the Statute, the Sanctions Board was composed of seven members, three of whom were selected from among the World Bank's senior staff by the World Bank President. The Sanctions Board reviews any allegations *de novo* on the basis of the written record before it. If requested, or if decided *sua sponte* by the Chair of the Sanctions Board, evidence may also be presented during a hearing. Final decisions made by the Sanctions Board, which describe the Board's reasoning in reaching the decision in detail, are posted on the World Bank's public website. Decisions of the Sanctions Board are non-appealable and the Sanctions Board has confirmed that it will only reconsider its decisions in narrowly defined and exceptional circumstances, such as the discovery of new and potentially decisive facts, fraud in the proceedings, and/or a clerical mistake in the original decision (Decision No. 62 ¶ 6 (January 2014); Decision No. 107 ¶ 4 (January 2018)).

2. Temporary Suspensions and Early Temporary Suspensions

In cases where the SDO recommends a sanction including a debarment exceeding a period of six months (which it does in most cases), the OSD will impose a temporary suspension on the respondent from the time the Notice of Sanctions Proceedings is issued through the final adjudication of the sanctions proceedings. Within 30 days of the delivery of the Notice of Temporary Suspension, the respondent may submit a written Explanation detailing why the Notice should be withdrawn.

If INT believes before it concludes its investigation into a respondent that there is sufficient evidence to support a finding of a sanctionable practice and that it is "highly likely" that the investigation will result in a SAE to be presented to the SDO within a period of one year, INT may submit a request for an Early Temporary Suspension to the SDO for approval. If the SDO then determines that there is sufficient evidence to support a finding that Respondent has engaged in a Sanctionable practice and that the accusations are such that the SDO would have recommended a debarment of at least two years, then the SDO shall issue the Notice of Temporary Suspension to the respondent.

An Early Temporary Suspension has an initial duration of six months, and, if at that time the SAE has not yet been submitted to the SDO, INT may request an extension of the Early Temporary Suspension by an additional six months. This extension request must be submitted no later than five months after the start of the temporary suspension and must (i) describe the current progress of the ongoing investigation and (ii) contain a representation that the investigation is ongoing and being pursued with "due diligence and dispatch." Upon submission of a SAE, the temporary suspension will be automatically extended until the end of the sanctions proceeding. The Sanctions Procedures set a relatively low standard for the imposition of Early Temporary

Suspensions, which—given their potential to cause irreversible economic damage before INT's investigation is even concluded—has been criticized as a potential violation of the concerned entity's general due process rights.

Like debarments imposed as part of a final decision, Temporary Suspensions and Early Temporary Suspensions render the respondent ineligible for World Bank contracts; however, they are not announced publicly. Instead, they are posted on the "Bank's Client Connection website" and shared only with the limited number of persons specified in the Sanctions Procedures. As a result, temporary suspensions do not trigger cross-debarment.

3. Settlements and Voluntary Disclosures

In addition to contested and uncontested sanctions proceedings, INT routinely resolves investigations through negotiated resolution agreements ("NRAs"). In fiscal year 2018, INT entered into 23 NRAs. INT and the respondent can enter into settlement discussions at any time during the investigation phase and even once the proceedings have begun. Depending on the terms of the NRA, the case can be closed, sanctions reduced or proceedings merely deferred pending compliance with specified conditions, which often includes ongoing cooperation (*i.e.*, providing INT with valuable information about potential misconduct, either by the cooperating party or other companies and individuals).

High-profile NRAs reached in the past include the February 2012 settlement with French engineering firm Alstom SA and the April 2013 settlement with Canadian giant SNC Lavalin. More recently, in January 2019, the World Bank announced that it had reached a settlement with Construtora Noberto Odebrecht S.A. ("CNO") in connection with fraudulent and collusive practices on the World Bank-funded Río Bogotá Environmental Recuperation and Flood Control Project in Colombia. CNO is a Brazilian construction and engineering subsidiary of Odebrecht S.A. and is the largest construction and engineering firm in Latin America. As part of the settlement, CNO agreed to a three year debarment with the requirement that it meet specific corporate compliance conditions—including the development of an integrity compliance program consistent with the World Bank Group Integrity Compliance Guidelines and full cooperation with INT going forward—in order to qualify for release from debarment and to acknowledge its responsibility for the Sanctionable Practices described by INT. The settlement agreement reflects a reduced sanction in recognition of CNO's cooperation and voluntary remedial actions, which included encouraging honest disclosures by employees, producing privileged documentation, and coordinating internal investigations with INT. The term of the settlement also triggers cross-debarment for CNO. As discussed further below, several other subsidiaries of Odebrecht also agreed in 2019 to settle charges with the Inter-American Development Bank.

B. AfDB Sanctions Regime

1. Investigation and Adjudication: Main Actors and Process

The AfDB's sanctions regime is comprised of one investigative body, the Office of Integrity and Anti-Corruption ("PIAC"), and a two-tiered adjudicatory system that includes the Sanctions Commissioner and Sanctions Appeals Board.

Office of Integrity and Anti-Corruption ("PIAC"): PIAC is the primary AfDB body charged with investigating and preventing Sanctionable Practices. PIAC is divided into two divisions, PIAC.1 (integrity and prevention division) and PIAC.2 (investigations division). PIAC.1 supports the Bank's mission by developing proactive measures that seek to decrease incidents of fraud and corruption. PIAC.2 is responsible for conducting investigations into allegations of Sanctionable Practices affecting the Bank's budget or a bank-funded project as well as allegations of misconduct by bank staff. Once PIAC.2 has concluded its investigation and has determined

to seek charges against a Respondent, it prepares a Finding of Sanctionable Practices that: (i) identifies the parties, (2) states the alleged Sanctionable Practices; (iii) provides a summary of relevant facts and grounds for the alleged Sanctionable Practices; (iv) proposes a sanction; and (v) includes all material information, including evidence supporting the allegations as well as exculpatory or mitigating evidence.

Sanctions Office: The Sanctions Office is headed by the Sanctions Commissioner and is the first-tier adjudicator for sanctions cases within the AfDB, reviewing the Findings of Sanctionable Practices submitted by PIAC.2. The Sanctions Commissioner is nominated by the AfDB President and is appointed by the Board of Directors of the Bank. The Sanctions Office is run administratively by the Sanctions Secretary. If the Sanctions Commissioner determines that the Findings of Sanctionable Practice supports a *prima facie* finding that Respondent has engaged in a Sanctionable Practice, the Sanctions Commissioner issues a formal Notice of Sanctions Proceeding ("Notice") to the Respondent, and notifies PIAC as well as the Sanctions Appeals Board and its Secretary. The Notice indicates, *inter alia*, to Respondent that Respondent has 60 days from receipt of the Notice to respond to the allegations in the Findings of Sanctions Practice and, if a temporary suspension has been issued, the manner in which Respondent may contest the Temporary Suspension. After the receiving Respondent's response (or if no response is submitted, solely on the basis of the Findings of Sanctionable Practices) the Sanctions Commissioner determines whether a "preponderance of the evidence" supports a finding that Respondent engaged in the Sanctionable Practice.

Sanctions Appeals Board: The Sanctions Appeals Board is the second-tier adjudicator of sanctions cases in the AfDB system and hears appeals from decisions made by the Sanctions Office. The Board consists of three members, including two external experts and one internal member, and several alternates. The two external members and two alternates are nominated by the Bank President and confirmed by the Board of Directors of the Bank. The one internal Sanctions Appeals Board member and one alternate are appointed directly by the Bank President from among the senior staff members of the Bank. The Bank also appoints a Secretary to the Appeals Board who reports to the Chairperson of the Board. A Respondent may appeal a Sanctions Decision made by the Sanctions Commissioner within 25 days. The Sanctions Appeals Board reviews the application *de novo* and Respondent may, as a result, present new evidence and arguments not presented in its Response. After receipt of the Appeal, the Sanctions Board forwards a copy to the PIAC and PIAC can submit a Reply. If PIAC includes new evidence or arguments in its Reply, Respondent can submit an additional rebuttal limited only to the new arguments or evidence made by the Reply. Unlike in the World Bank's sanctions regime, Respondents have no right to a hearing in front of the AfDB Sanctions Appeals Board. The Board can, however, hold a hearing on the request of either the Respondent or PIAC, or *sua sponte* if it so chooses. The form, length, and nature of the hearing are likewise determined by the Board.

2. Temporary Suspensions

Although the AfDB also allows for Temporary Suspensions, it imposes a stringent standard for their implementation. The AfDB procedures specify that PIAC may submit a request for a Temporary Suspension at the time the Findings of Sanctionable Practices is presented, or for an Early Temporary Suspension prior to the conclusion of an investigation. Temporary Suspensions, however, will only be granted if the "continuous eligibility of the subject of the investigations would cause imminent financial or reputational harm" to the AfDB. Requests for Early Temporary Suspensions require a showing by PIAC of "sufficient evidence to indicate a likelihood that the Respondent has engaged in a Sanctionable Practice." In cases where an Early Temporary Suspension has been requested, Respondents may submit an Objection to the Temporary Suspension to the Sanctions Commissioner.

3. Settlements

Under the AfDB's Sanctions Procedures, at any time prior to the issuance of a Final Decision, PIAC and the Respondent can agree to a Negotiated Settlement. PIAC and the Respondent may also request a stay of proceedings to conduct settlement negotiations. All settlement agreements must be approved by the AfDB General Counsel—who reviews the agreement to ensure that the agreement does not violate the AfDB's policies and procedures—and by the Sanctions Commissioner—who reviews the agreement to ensure fairness, transparency, and credibility.[37]

The AfDB concluded its first set of negotiated settlement agreements in early 2014 and since then has continued to be open to settling with contractors. In December 2015, for example, the AfDB reached a settlement with Tokyo-based multinational conglomerate Hitachi, ending the AfDB's three-year investigation into allegations of sanctionable practices by certain Hitachi subsidiaries on a power station contract in South Africa. The settlement included the subsidiaries' debarment for one year in exchange for an undisclosed but—according to the press release—"substantial" financial contribution by Hitachi to the AfDB. This case presents a prominent illustration of cooperation between MDBs and national enforcement authorities. The AfDB shared information obtained in the course of its three-year investigation with the U.S. SEC, which, in turn, launched its own investigation into the matter. The SEC's investigation was settled in September 2015, with Hitachi agreeing to pay $19 million in civil penalties.

More recently in May 2018, the AfDB debarred Chinese company CHINT Electric for 36 months (with an opportunity for early release after 24 months) under a negotiated settlement for fraudulent practices on multiple AfDB-funded projects. According to the AfDB's announcement, in multiple bids, CHINT misrepresented its prior experience in order to meet qualification requirements. The AfDB indicated that CHINT's release from debarment is conditioned on adoption of a comprehensive integrity compliance program that meets the standards of the AfDB.

C. Inter-American Development Bank Sanctions Regime

First adopted in 2001 and updated in 2011 and 2015, the Inter-American Development Bank ("IDB") sanctions system features a two-tiered sanctions process overseen by the IDB's Office of Institutional Integrity ("OII"), Sanctions Officer, and Sanctions Committee. In accordance with the General Principles and Guidelines for Sanctions and the Uniform Framework for Preventing and Combating Fraud and Corruption, the IDB's sanction system investigates and prosecutes the five standard sanctionable practices, referred to as Prohibited Practices by IDB, agreed to as part of the Joint International Financial Institution Anti-Corruption Task Force's harmonization efforts in 2006.

1. Investigation and Adjudication: Main Actors and Process

Office of Institutional Integrity: OII is an independent advisory office within the IDB responsible for investigation allegations of fraud, corruption, and other Prohibited Practices in IDB-financed activities. OII also plays a primary role arranging Negotiated Resolution Agreements ("NRAs"), discussed in further depth below. OII also provides consultations on risk indicators and mitigation measures for operational staff working on IDB-financed projects and conducts Integrity Risk Reviews ("IRR") of specific projects, sectors, or topics to identify and assess integrity risks. Under the IDB's two tiered process, if OII determines after its investigation that charges are warranted, it issues a Statement of Charges to be reviewed by the Sanctions Officer. The Statement of Charges includes: (i)

37. AfDB Sanctions Procedure, § 15.1, 15.3.

the identity of each party alleged to have engaged in a prohibited practice; (ii) the alleged prohibited practice; (iii) a summary of the relevant facts on which the allegations are based; (iv) all evidence relevant to the determination of the sanction in the possession of OII; (v) all exculpatory or mitigating evidence in the possession of OII; and (vi) any other information that OII determines to be relevant to the Statement of Charges.

Sanctions Officer: The Sanctions Officer acts as the primary adjudicator of IDB sanctions proceedings, determining based on OII investigations whether or not the uncovered evidence supports the allegation of Prohibited Practices and determining what sanction may be appropriate for the situation. If the Sanctions Officer agrees that the investigated party engaged in the alleged Prohibited Practice, it issues a Notice of Administrative Action ("NAA") to the Respondent indicating that sanctions proceedings have been initiated. The NAA contains a copy of the Statement of Charges, the findings of the Sanctions Officer, and a copy of the Sanctions Procedures, as well procedural documents informing the Respondent that it has the opportunity to respond and that the IDB may impose a range of sanctions.

After receipt of the NAA, the Respondent may submit a written Response to the Sanctions Officer. The OII may also submit additional information to the Sanctions Officer, who may then require additional clarifications or evidence from the Respondent and from the OII. After reviewing all evidence and submissions, the Sanctions Officer issues its determination as to whether or not the Respondent has engaged in the alleged Prohibited Practice(s) and what punishment should be imposed. If no Response is received within the 60-day period, the Respondent is judged to have admitted the allegations and to have waived its opportunity to appeal to the Sanctions Committee. After expiration of the 60-day period, the Sanctions Officer re-assesses the submission of OII and the Respondent and shall issue a Determination either dismissing the allegations or finding that a preponderance of the evidence supports the finding that the Respondent engaged in the Prohibited Practice and imposing sanctions on the Respondent.

While the Determination of the Sanctions Officer is appealable to the Sanctions Committee, OII reports that the number of cases that are appealed has decreased in recent years from over 40% in 2015 to under 19% in 2017 and 0% in 2018.

Sanctions Committee: The Sanctions Committee is the final adjudicatory body in the IDB sanctions regime and consists of three IDB staff members, four external members, and one alternate member who represents the Inter-American Investment Corporation, the IBD's private sector lending arm. The Sanctions Committee reviews appeals from the Sanctions Officer's determinations on a *de novo* basis using a preponderance of the evidence standard. The Sanctions Committee is also not bound by the sanction decided by the Sanctions Officer and is free to impose a different sanction or no sanction at all.

Following the Sanctions Officer's Determination, the Respondent has 45 days to file a written appeal with the Executive Secretary of the Sanctions Committee. OII may submit additional written materials in reply to Respondent's appeal. As in the AfDB system, the Sanctions Committee may hold hearings as it deems appropriate, but neither OII nor the Respondent have the right to a hearing in front of the Sanctions Committee. The Sanctions Committee's Decision is final and cannot be further appealed aside from in certain limited circumstances.

2. Temporary Suspensions

OII can request Temporary Suspensions at any time from the initiation of the investigation, and such suspensions may extend through the final decision of the Sanctions Committee. If imposed, the Sanctions Officer must send written notice to the Respondent and to OII (a "Notice of Temporary Suspension") which includes the recommendation for Temporary Suspension as well as a summary of the basis for the Sanctions Officer's

decision. This information may be included in the NAA if the Temporary Suspension is implemented at the same time that the Sanctions Officer delivers this notice to the Respondent.

As under the AfDB system, to impose a Temporary Suspension the Sanctions Officer must find, in consultation with the Chairperson of the Sanctions Committee, that the subsequent award of contracts to the Respondent "could result in significant harm" to the IDB or to IDB-financed projects and that OII has "substantial evidence" that supports the allegation of Prohibited Practice. The Respondent may submit a written Request for Reconsideration to the Sanctions Officer within 20 days following delivery of the Notice of Temporary Suspension. The Temporary Suspension has an immediate effect upon delivery of the Notice of Temporary Suspension and may last for up to 12-months or until the allegations are ultimately resolved through dismissal or sanction. Temporary Sanctions may be extended for additional 12-month periods on the recommendation of OII and approval of the Sanctions Officer, in consultation with the Chairperson of the Sanctions Committee.

3. Negotiated Resolutions

The Sanctions Procedures, as amended in 2015, authorize the IDB to enter into Negotiated Resolution Agreements ("NRAs") with investigated parties at any point prior to the receipt of the Statement of Charges by the Sanctions Officer. OII has indicated that it generally only employs NRAs in cases involving complex investigations where the investigated parties are able to and willing to provide information to the IDB about the (i) alleged Prohibited Practices and systematic risks in the affected operations or (ii) significant Prohibited Practices of the investigated party or other parties. This information is valued because it provides a full picture of the integrity risks facing IDB-financed activities, including details about agencies and individuals that may help the bank's operational teams to better manage these risks in the future. OII reported that in 2018 it negotiated three NRA engagements and concluded one—with Odebrecht S.A.—that marked its first ever use of the NRA tool.

In September 2019, IDB announced that it had agreed to its first-ever NRA with Brazilian construction conglomerate Odebrecht S.A. following an extensive investigation by OII. OII's investigation revealed, and as part of the NRA Odebrecht did not contest, that between 2006 and 2008 Odebrecht paid approximately $380,000 in bribes to Brazilian officials in relation to the Highway Rehabilitation Program in the State of São Paulo and that between 2007 and 2015 it paid approximately $118 million through a network of agents and offshore accounts to Venezuelan officials in relation to the Tocoma Hydroelectric Power Plant Program. The NRA includes a six-year debarment followed by a four-year conditional non-debarment for Odebrecht's subsidiary CNO S.A. (and 19 of its subsidiaries) and a ten-year conditional non-debarment for Odebrecht's subsidiary Odebrecht Engenharia e Construção S.A. ("OEC") (and 41 of its subsidiaries). Odebrecht also committed, starting in 2024, to paying the $50 million to NGOs and charities dedicated to managing social projects intended to improve the quality of life for vulnerable communities in IDB's development member countries. The NRA also requires that Odebrecht engage an independent compliance monitor to report on its compliance program to the IDB.

4. Recent Resolutions

As of January 2019, the IDB began to publish short summaries of case decisions by the Sanctions Officer and the Sanctions Committee in order to improve accountability and transparency of the sanctions adjudication process. To date, it has posted summaries of seven Determinations made by the Sanctions Officer against Respondents involved in a consortium in Peru. All Respondents were found to have committed Fraudulent Practices, with sanctions ranging from debarment of four years to a debarment of one year with an additional three years of conditional non-debarment. None of these cases appear to have been appealed to the Sanctions Committee and no summaries of Sanctions Committee decisions have been posted.

D. Other MDB Sanctions Regimes: Highlights

A number of other MDBs have also implemented sanctions regimes based on the World Bank model. Select highlights of these regimes are presented below.

European Bank for Reconstruction and Development: Sanctions procedures at the EBRD are governed by the "Enforcement Policy and Procedures." Under these procedures, EBRD has adopted a two-tiered adjudicatory process, with an initial review by the "Enforcement Commissioner" and a second level review by an "Enforcement Committee," made up of five members (three external to the EBRD). Decisions of the Enforcement Committee are final and no longer subject (as before) to the referral to the Bank's President or Executive Committee. EBRD's investigative body is the Office of the Chief Compliance Officer. The Office of the Chief Compliance Officer has the authority to bring formal sanctions proceedings or enter into negotiated resolution agreements.

Asian Development Bank: Like many of the other MDBs, the Asian Development Bank's Integrity Principles and Guidelines ("Guidelines") are built around an investigative body—the Office of Anticorruption and Integrity ("OAI")—and two adjudicative bodies—the Integrity Oversight Committee and the Sanction Appeals Committee. In order to ensure greater independence from the investigation process, the Guidelines mandate that the Sanctions Appeals Committee's chair be picked from senior ADB staff, external to the OAI. Unlike many of its peers, the ADB has decided not to move towards a full publication of its sanctions decisions. Instead, the ADB publishes high-level (and anonymous) summaries of its sanction cases and maintains its rule that the identity of first time offenders is not publicized, unless limited exceptions apply (e.g.*,* failure to respond to notice of proceedings, failure to acknowledge debarment decision, etc.). Accordingly the ADB's published sanctions list contains the names of entities and individuals who violated the sanctions while ineligible, entities and individuals who committed second and subsequent violations, debarred entities and individuals who cannot be contacted, and cross-debarred entities and individuals.

AIIB: The AIIB's sanctions process is set out in the Policy on Prohibited Practices, which was released on December 8, 2016. The AIIB's process is largely modeled on the World Bank's system and provides for a two-tiered adjudicatory system. At the first stage, the AIIB's investigative body, the Compliance, Effectiveness and Integrity Unit (CEIU), headed by a Director General, is tasked with investigating suspected misconduct. Investigations Officers look into suspicious activities and make recommendations to a Sanctions Officer, who in turn decides whether charges are supported using a preponderance of evidence standard. Respondents have an opportunity to contest the Sanctions Officer's findings before he makes a final determination and imposes sanctions. At the second stage, respondents can appeal the Sanctions Officer's determination to the Sanctions Panel. The Panel is composed of three members, one internal and two external, who are appointed by the Bank's President. As mentioned above, in 2017, the AIIB voluntarily adopted the MDB's cross-debarment list and announced its intention to formally apply for inclusion in the MDB's Cross-Debarment Agreement.

III. Useful Lessons from World Bank Sanctions Board's Decisions

The World Bank has historically been the only MDB to publish the decisions of its final adjudicative body in full text. The growing body of World Bank Sanctions Board decisions is of particular value, as the decisions set out, in detail, the Board's sanctioning analysis, especially with respect to the initiatives and remedial actions that it expects from companies and individuals to receive mitigating credit. These mitigation factors are discussed in every Sanctions Board decision. Of similar practical importance to many companies working on World Bank and other MDB-funded projects, the Sanctions Board released a decision in 2017 that provides a rare insight into its understanding of successor liability.

A. Mitigation of Potential Sanctions

An analysis of published Sanctions Board decisions shows that the mitigation accorded by the Sanctions Board can indeed be meaningful. For example, in one decision, the proposed sanction of a three-year debarment with conditional release (which corresponds to the Bank's "baseline" sanction) was reduced to a six month retroactive, non-conditional debarment in large part due to a multitude of mitigating factors (Decision No. 63 ¶¶ 106-107, ¶¶ 109-110, ¶ 112 (January 2014).) The significance of mitigation credit is also evident from the increased sanctions levied when such factors are absent. (*See*, e.g., Decision No. 69 ¶¶ 39, 41, 45 (June 2014).)

1. Lessons from Recent Cases

a. Employee Discipline

The Sanctions Board has long placed emphasis on disciplining responsible employees. The Sanctions Board will only provide mitigating credit if such disciplining is the result of an adequate inquiry into the matter (rather than provoked by a desire to find a convenient scapegoat). Accordingly, the Sanctions Board has declined to provide mitigation credit to companies that (i) disciplined a responsible employee without thoroughly investigating the underlying conduct to allow the company to "assess and address its own responsibility or that of other employees" (Decision No. 55 ¶ 77 (March 2013)) or (ii) did not provide any "proof of a demonstrable nexus" between the relevant employee's departure/disciplining and the sanctionable conduct at issue. (Decision No. 56 ¶ 67 (June 2013))

A recent Sanctions Board decision confirmed that respondents must be prepared to present evidence and specifics regarding employee discipline. Broad assertions that appropriate measures have been taken and that specific staff have been disciplined must be supported by documentary evidence to receive mitigation credit. (Decision No. 117, ¶35 (April 2019)).

Moreover, the Sanctions Board has been clear that, to receive mitigating credit, the corrective actions have to target the staff actually involved in the misconduct. In one of the decisions, the respondent claimed mitigating credit for having filed a police report and terminating its relationship with the agent who had issued allegedly forged bid securities; neither of which—the Sanctions Board found—addressed misconduct arising "within the Respondent's own staff or operations." (Decision No. 67, ¶ 39 (June 2014).) In another decision, the respondent claimed mitigating credit for having issued a warning letter against its finance and deputy finance director. The Sanctions Board again denied mitigating credit on the basis that no disciplinary measures were taken against the marketing staff, which had allegedly processed the tender, as well as (lower-echelon) finance staff, which had processed the bid securities. (Decision No. 68 ¶ 39 (June 2014)) Most recently, the Sanctions Board made clear that respondents must be willing to discipline even senior staff involved. The Sanctions Board provided only limited mitigation credit to a respondent that disciplined junior employees involved in the misconduct but suspended a Deputy Chairman for only 10 days. (Decision No. 116, ¶ 25 (March 2019)).

b. Compliance Programs

The existence of a compliance program has long been one of the key areas of inquiry for the Sanctions Board. If an employer can demonstrate to the Sanctions Board's satisfaction that it had implemented, prior to the conduct at issue, controls reasonably sufficient to prevent or detect the conduct, the employer would appear to have a defense against liability for its employees' actions. For companies that have or may seek World Bank Group–financed contracts, these decisions create a substantial incentive to review and, as necessary, recalibrate existing

compliance programs to both anticipate likely compliance risks and generally meet the World Bank's expectations for compliance programs.

The Sanctions Board also gives credit for compliance program modifications implemented in response to alleged misconduct. Even if a pre-existing compliance program had not been reasonably designed to prevent or detect the conduct at issue, the Sanctions Board has indicated that it will also provide mitigation credit for post-conduct compliance modifications designed to prevent or detect the recurrence of the alleged misconduct. (Decision No. 51 ¶¶ 51-52 (May 2012); No. 53 ¶¶ 60-61 (September 2012), No. 60 ¶¶ 129-30 (September 2013). Limited compliance enhancements, on the other hand, lead to lesser credit. In one decision, the Sanctions Board agreed to provide "some mitigating credit, limited by the lack of more evidence" for the adoption of a company-wide prohibition against misconduct with approval and support of senior management. (Decision No. 56 ¶¶ 68-69 (June 2013).) Unit or department-level improvements can also result in some mitigation credit. (Decision No. 55 ¶ 78 (March 2013).)

Moreover, recent Sanctions Board decisions indicate that the responsiveness with which these remedial actions are implemented matters. In the past, the Sanctions Board has given significant weight to modifications that have been made prior to the issuance of the Notice of Sanctions Proceedings to respondents (Decision No. 63, ¶ 107 (January 2014), No. 71, ¶ 94 (July 2014), No. 79, ¶¶ 46 (August 2015)). Recently, the Sanctions Board has determined that delays in remediation can and will result in less mitigation credit. In Decision 120, where the respondent did not take remedial measures until two years after the respondent indicated it would, the Sanctions Board interpreted the delay to mean that the compliance reforms were "driven more by a desire for sanction mitigation than by genuine remorse or intent to reform" and awarded only partial mitigation credit as a result. (Decision No. 120, ¶56 (May 2019)).

Recent Sanctions Board decisions also confirm that respondents may be required to provide evidence to support statements that particular compliance processes have been improved or strengthened. For example, in Decision No. 78, the Sanctions Board required a respondent to provide evidence to support an assertion that its third party due diligence process had been improved. (Decision No. 117, ¶ 36 (April 2019).

c. Time Since the Misconduct

Recent decisions from the Sanctions Board have confirmed that mitigation credit will be available to respondents for the passage of significant amounts of time between when an offense occurred and when the sanctions proceedings is initiated. The Sanctions Board has stated that this factor weighs on "the fairness of the process for respondents" and that it will affect the weight that the Sanctions Board attaches to the evidence presented. Despite the fact that the Sanctions Procedures provide for a 10-year statute of limitations, the Sanctions Board has recently found that delays of six and a half years (Decision No. 121, ¶ 23 (May 2019)), four and a half years (Decision No. 118, ¶ 90 (April 2019)), five years (Decision no. 114, ¶ 64 (Nov. 2018)), and six years and four months (Decision No. 113, ¶ 47 (Nov. 2018)) between the occurrence of the misconduct and the initiation of sanctions proceedings were enough to have merited mitigation credit in what appears to be an effort to spur speedier investigations and processing from INT. While the impact of each specific mitigation factor on the overall sentence is not discussed by the Sanctions Board and cannot be easily divined, in many of the cases where the Sanctions Board found that the passage of time warranted mitigation credit, the respondent received a marked decrease from the SDO's recommended sanction. Recent examples include a recommended three-year debarment with conditional release reduced to a letter of reprimand (Decision No. 121, ¶ 35 (May 2019)) and a recommended eleven-year and two-month debarment with conditional release reduced to a four-year and six-month debarment with conditional release. (Decision No. 118, ¶ 93 (April 2019)).

2. Other Mitigating Factors

In addition to the above, the Sanctions Board has long valued and credited the respondents' cooperation with INT and own efforts to conduct an internal investigation.

a. Cooperation with INT

The Sanctions Board will give companies and individuals mitigating credit if they cooperate during the course of the investigation conducted by INT. Interestingly, such mitigation credit can be obtained even when the company does not comply with *all* of INT's requests (Decision No. 79 ¶ 48 (August 2015), mentioning "gaps" in the company's responses to INT's queries). More noteworthy still are instances where the concerned companies were accused of initially obstructing INT's investigation. For instance, in Decision No. 60, the Sanctions Board found select respondents culpable of obstruction for having ordered the deletion of emails before INT's audit. Ultimately, however, these respondents were awarded "significant" mitigating credit for having (i) met with INT and admitted misconduct; (ii) provided inculpatory evidence and (iii) made efforts to retrieve previously deleted emails. (Decision No. 60, ¶ 133 (September 2013).) Similarly, in Case No. 63, the Sanctions Board found that attempts by a respondent entity's employees to interfere with INT's investigation warranted aggravation, while also applying mitigation for subsequent efforts by respondent entity's management to correct the employee's actions. (Decision No. 63, ¶¶ 102 and 110 (January 2014).)

Moreover, in another decision, the Sanctions Board made it clear that it will not necessarily link the mitigating credit accorded to a cooperating company to the success of the investigation conducted by INT. In this particular decision, the Sanctions Board granted mitigation to a Respondent Director who participated in two interviews with INT, despite the fact that these interviews did not shed light on an area of particular relevance to the case. Indeed, the Sanctions Board noted the lack, in the record, of any indication that INT had asked questions pertaining to these relevant areas. It would therefore appear that the responsibility for successful cooperation lies not only with the respondents but also with INT. (Decision No. 73 ¶ 48 (October 2014).)

b. Internal Investigations

Companies will also be given mitigation credit when they take the initiative to conduct their own internal investigation into the alleged misconduct. Here, it is important to note that the Sanctions Board expects (and will only give mitigating credit if) such internal investigations are undertaken by persons with sufficient independence, expertise, and experience. (Decision No. 50 ¶ 67 (May 2012).) The Sanctions Board has clarified that the burden to prove the independence of internal investigators lies with the respondents: in Decision No. 68, the Board refused to apply mitigation where a respondent had claimed that its "Board of Management" had conducted an internal investigation without specifying the composition of the Board or speaking to the independence of its members. (Decision No. 68, ¶ 43 (June 2014).)

The Sanctions Board also expects internal investigations to be adequately documented and credibly performed and that such investigations lead to concrete and targeted follow-up actions, when appropriate (for denial of mitigation on these grounds, see Decision No. 71, ¶¶ 98-100 (July 2014) and Decision No. 77, ¶ 56 (June 2015). Importantly, the Sanctions Board notes positively and accords mitigating credit when the results of an internal investigation are shared with INT and/or relevant national authorities. (Decision No. 63, ¶112 (January 2014).) However, companies sharing such information should be cognizant of the potential implications, and, in particular, of the possibility of parallel proceedings, discussed *infra*.

IV. International Cooperation and Referrals

Companies and individuals participating in MDB-financed projects should be aware that sanctions proceedings before an MDB do not occur in a vacuum. Instead, there has been a growing trend for increased cooperation and information sharing among MDBs and between MDBs and international and national anti-corruption enforcement authorities, which can lead to parallel proceedings. Such increased cooperation is made possible through various tools. For example, to date, the World Bank has signed over 55 cooperation agreements with national and international enforcement authorities (including with the U.K. Serious Fraud Office, the European Anti-Fraud Office, the UN Office for Internal Oversight and the International Criminal Police Organization (INTERPOL)) in support of parallel investigations, information sharing and asset recovery.

Moreover, most MDB sanctions procedures contain so-called referral clauses, which allow the MDBs in question to share information about potential sanctionable practices with other MDBs and/or international and national prosecuting authorities. In the 2018 fiscal year, the World Bank itself referred 43 cases to national authorities and other MDBs. In total, as of the end of fiscal year 2018, the Bank has made 499 referrals to anti-corruption bodies in countries all over the globe. As discussed below, the effects of such increased cooperation are wide-reaching, and the two-way information sharing leads to national procedures “spilling over” into MDB sanctions procedures and vice versa.

A. Referrals from National Authorities to MDBs

Information shared by national authorities can help MDBs substantiate allegations of sanctionable practices while an investigation is still ongoing. National authorities can also refer information after an investigation has been closed and the sanctions proceedings are underway. This was poignantly (and dramatically) illustrated by Sanctions Board Decision No. 72. The case underlying this 2014 decision arose in connection with two World Bank-funded projects in Iraq, for which respondents submitted successful bids with the assistance of a local agent. Among other things, INT alleged that respondents engaged in corrupt practices by offering and/or paying the agent a commission with the expectation that these funds would be used to influence procurement officials working on the projects. Respondents rejected the allegations. However, two days before the scheduled hearing before the Sanctions Board, INT obtained its evidentiary *pièce de résistance* through a referral by Iraqi national authorities, who shared with INT email correspondence in which the agent clearly stated that part of the commission would be used to make payments to a project manager. Largely based on this evidence, the Sanctions Board proceeded to debar the concerned respondents for four years, a dramatic increase from the one-year debarment with conditional release proposed by the SDO.

B. Referrals from MDBs to National Authorities

The Sanctions Board decision involving Dutch company Dutchmed BV highlights the tension that can arise between an MDB’s contractual audit rights, the MDB’s practice of referring matters to national authorities, and a respondent’s potential rights against self-incrimination. On June 2, 2017, the World Bank Group Sanctions Board imposed a fourteen-year debarment on Dutchmed BV and its affiliates for five counts of corrupt practices and one count of obstructive practices in connection with a Bank-funded Health Sector Reform Project in Romania.

According to the decision, the respondent made corrupt payments to secure approximately $10 million worth of contracts, including illicit commissions to a procurement advisor and personal trips for personnel of a project management unit. INT also claimed that the respondent obstructed its investigations by materially impeding its audit and inspection rights and refusing access to its records. At the first tier of the sanctions regime, the Suspension and Debarment Officer found against the respondent and imposed a ten-year debarment.

The respondent appealed to the Sanctions Board, claiming that INT failed to establish the elements of corruption, and that its inability to cooperate stemmed from exercise of its right against self-incrimination under Article 6 of the European Convention on Human Rights. According to the company, based on its status as a suspect in national criminal proceedings, compliance with INT's request for unconditional cooperation would have impaired its exercise of this privilege in future prosecutions. Given the prolific nature of the World Bank's referral practices, the fear of self-incrimination may have had some merit. As of December 2016, INT's referrals had resulted in prosecution and conviction of at least 35 individuals and criminal charges against another 29 parties.

The Sanctions Board nevertheless found against the respondent on all counts. On the obstruction charge, the Board highlighted the contractual nature of INT's audit and inspection rights, distinguishing between the Bank's administrative proceedings and external criminal proceedings.

For more information, please contact:

KEVIN T. ABIKOFF
+1 (202) 721-4770
kevin.abikoff@hugheshubbard.com

LAURA N. PERKINS
+1 (202) 721-4778
laura.perkins@hugheshubbard.com

hugheshubbard.com